

542,014

特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2004 年 8 月 19 日 (19.08.2004)

PCT

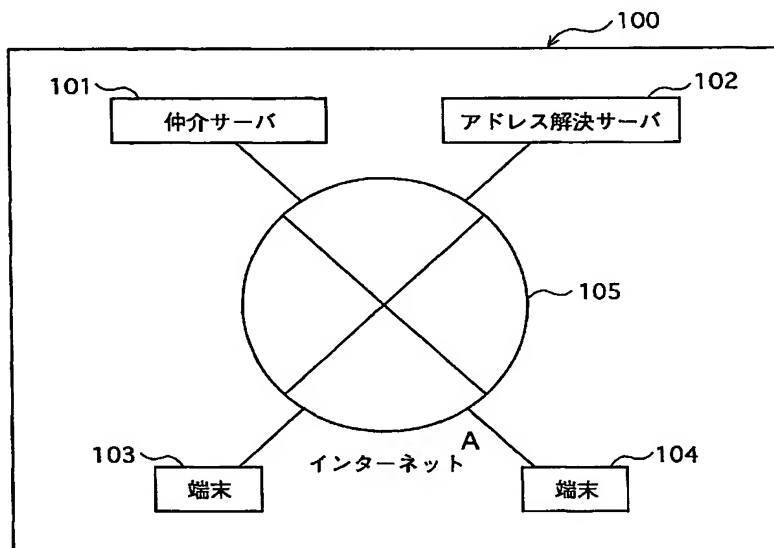
(10) 国際公開番号  
WO 2004/071037 A1

- |                            |                                |   |
|----------------------------|--------------------------------|---|
| (51) 国際特許分類 <sup>7</sup> : | H04L 12/66                     | (71) 出願人 (米国を除く全ての指定国について): 松下電<br>器産業株式会社 (MATSUSHITA ELECTRIC INDUS-<br>TRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大<br>字門真 1006 番地 Osaka (JP). |
| (21) 国際出願番号:               | PCT/JP2004/001099              |   |
| (22) 国際出願日:                | 2004 年 2 月 4 日 (04.02.2004)    | (72) 発明者; および   |
| (25) 国際出願の言語:              | 日本語                            | (75) 発明者/出願人 (米国についてのみ): 宗 續 敏<br>彦 (MUNETSUGU, Toshihiko) [/]. 長 友 健 一 (NA-<br>GATOMO, Kenichi) [/]. 安 部 美 乃 夫 (ABE, Minobu)<br>[/].           |
| (26) 国際公開の言語:              | 日本語                            |   |
| (30) 優先権データ:               |                                | (74) 代理人: 中島 司朗 (NAKAJIMA, Shiro); 〒5310072 大<br>阪府大阪市北区豊崎 3 丁目 2 番 1 号 淀川 5 番館 6F Osaka<br>(JP).   |
| 特願 2003-027677             | 2003 年 2 月 4 日 (04.02.2003) JP |   |

[続葉有]

(54) Title: COMMUNICATION SYSTEM, AND COMMUNICATION CONTROL SERVER AND COMMUNICATION TERMI-  
NALS CONSTITUTING THAT COMMUNICATION SYSTEM

(54) 発明の名称: 通信システム及び当該通信システムを構成する通信制御サーバ及び通信端末



101...INTERMEDIATE SERVER  
102...ADDRESS SOLVING SERVER  
103...TERMINAL  
A...INTERNET  
104...TERMINAL

(57) Abstract: A communication system (100) comprises terminals (103,104) and an intermediate server (101) that notifies destination information for determining the address of the second communication terminal on the network. The terminal (103) transmits to the intermediate server (101) a request message for requesting for the destination information. The intermediate server (101) comprises a storage part (206) that has stored a permitted-terminal table indicative of correspondence between the terminal (104) and a terminal permitted to be connected with the terminal (104); a reception part (203) for receiving the request message; and a control part (201) for determining, based on the permitted-terminal table, whether the terminal (103) that has transmitted the received request message is a terminal permitted, by the terminal (104), to be connected with the terminal (104), and for notifying the terminal (103) of the destination information of the terminal (104) only if the terminal (103) is a terminal permitted to be connected with the terminal (104).

(57) 要約: 端末 103 及び端末 104 と、第 2 通信端末のネットワーク上におけるアドレスを特定するための宛先情報を通知する仲介サーバ 101 とから構成される通信システム 100 であって、端末 103 は、前記宛先情報を要求する要求メッセージを仲介サーバ 101 に送信し、仲介サーバ 101 は、端末 104 と、端末 104 への接続が許可された端末との対応関係を示す許可端末テーブルを記憶している記憶部 206 と、前記要求メッセージを受信する受信部 203 と、受信した前記要求

[続葉有]

WO 2004/071037 A1



(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL,

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

メッセージを送信した端末103が、端末104によって接続が許可されている端末であるか否かを、前記許可端末テーブルに基づいて判定し、端末103が接続が許可されている端末である場合に限り、端末104の宛先情報を、端末103に通知する制御部201とを有することを特徴とする通信システム。

## 明 細 書

通信システム及び当該通信システムを構成する通信制御サーバ及び通信  
端末

## 5 技術分野

本発明は、通信回線で接続される端末間の通信制御を行なう通信システム、及び当該通信システムにおける通信制御方法、及び当該通信システムを構成する通信制御サーバ、通信端末に関する。

## 10 背景技術

近年、通信ネットワークインフラの発達によって、多数のユーザがインターネットに接続するようになった。また、DSLやケーブルモデム、光ファイバといった高速アクセスリンクの普及により、広帯域でのネットアクセスが可能となった。

- 15 また、インターネットに接続する端末にも、様々な新しい種類の端末が開発され、例えば、テレビやハードディスク内蔵ビデオレコーダなど家電製品でもインターネットを利用するものが開発されている。さらに、インターネットの利用形態においても、従来のサーバクライアント方式のサービスに加えて、ユーザの端末同士が直接通信するピアツー  
20 ピア (Peer to Peer) 方式の利用形態のサービスが利用できるようになっている。

- 一般的に、ネットワークサービス加入者が利用する端末では、PPP (Point to Point Protocol)、PPPoE (PPP over Ethernet) などを用いることにより、IPアドレスがインターネット接続時に動的に割り  
25 当てられる。そのため、接続のたびにIPアドレスは変化する。

したがって、端末間でピアツーピアに接続を行う場合、その時点で端末に割り当てられているIPアドレスを取得する仕組みが必要となる。この問題を解決するための従来技術として、後述する特許文献1及び2が開示されている。

これにより、ダイヤルアップ接続等によりインターネットに接続されたユーザー端末に対して、他のユーザー端末が不具合を生じることなく、接続することができ、ユーザー端末同士の通信を容易に確立することができる。

- 5      しかしながら、上記のようなユーザー端末同士の通信においては、インターネットに接続されたユーザー端末に対して、そのIPアドレスを指定することにより、どこからでもアクセス可能になるため、当該ユーザーが意図していない者からのいたずら目的の接続など、当該ユーザーにとって不都合な接続がなされてしまうという問題が生じる。

10

#### 発明の開示

本発明は、上記問題に鑑み、ユーザー端末同士の通信において、他のユーザー端末からの不都合な接続を有効に防止する、通信制御サーバ、通信端末、及び通信システムを提供することを目的とする。

- 15      上記目的を達成すべく、本発明は、第1及び第2通信端末と、第2通信端末のネットワーク上におけるアドレスを特定するための宛先情報を通知する通信制御サーバとから構成される通信システムであって、第1通信端末は、前記宛先情報を要求する要求メッセージを前記通信制御サーバに送信し、前記通信制御サーバは、第2通信端末と、第2通信端末への接続が許可された接続許可通信端末との対応関係を示す許可端末テーブルを記憶している許可端末テーブル記憶手段と、前記要求メッセージを受信する要求メッセージ受信手段と、受信した前記要求メッセージを送信した第1通信端末が、第2通信端末に対応付けられている接続許可通信端末に該当するか否かを、前記許可端末テーブルに基づいて判定する
- 20      端末判定手段と、第1通信端末が第2通信端末に対応付けられている接続許可通信端末に該当する場合に限り、第2通信端末の宛先情報を、第1通信端末に通知する通知制御手段とを有する。

ここで、前記アドレスは、IPアドレスであることとしてもよい。

ここで、前記アドレスは、IPアドレスとポート番号とから構成され

ることとしてもよい。

又、本発明は、通信端末のアドレスを特定するための宛先情報を通知する通信制御サーバであって、前記通信端末と、当該通信端末への接続が許可された通信端末との対応関係を示す許可端末テーブルを記憶している許可端末テーブル記憶手段と、前記宛先情報を要求する要求メッセージを要求元通信端末から受信する要求メッセージ受信手段と、前記要求元通信端末が、前記通信端末に接続を許可されている通信端末であるか否かを、前記許可端末テーブルに基づいて判定する端末判定手段と、前記要求元通信端末が、接続を許可されている通信端末である場合に限り、前記通信端末の宛先情報を前記要求元通信端末に通知する通知制御手段とを備えることとしてもよい。

これにより、予め接続が許可されている通信端末に対してのみ、接続に必要な宛先情報が通知されるので、通信端末の利用者は、自己が意図していない利用者からの接続を有効に防止することができる。

ここで、前記通信システムにおいて、前記通知制御手段はさらに、第1通信端末が第2通信端末への接続が許可されている通信端末である場合に限り、第2通信端末が第1通信端末を認証するための認証情報を作成する認証情報作成手段を有し、前記通知制御手段はさらに、前記認証情報を、第1通信端末と第2通信端末に通知し、第1通信端末は、第2通信端末への接続要求時に、通知された認証情報を第2通信端末に送信し、第2通信端末は、第1通信端末から前記認証情報を受信する受信手段と、受信した認証情報と通知された認証情報とが一致するか否かを判定する判定手段と、両者の認証情報が一致する場合に限り、第1通信端末からの接続を許可する接続制御手段とを有することとしてもよい。

又、本発明は、通信制御サーバとネットワークで接続された通信端末であって、前記通信制御サーバに、前記通信端末への接続が許可された通信端末の登録要求をする許可通信端末登録要求手段と、前記通信端末のネットワーク上におけるアドレスを特定するための宛先情報を要求した通信端末が前記通信端末への接続が許可された通信端末である場合に

限り、前記通信制御サーバから送信される、前記宛先情報を要求した通信端末を認証するための認証情報を受信する認証情報受信手段と、前記宛先情報を要求した通信端末から、接続受入要求と当該通信端末を識別するための識別情報を受信する識別情報受信手段と、前記認証情報と前記識別情報とが一致するか否かを判定する判定手段と、前記認証情報と前記識別情報とが一致する場合に限り、前記宛先情報を要求した通信端末からの接続受入要求に基づく接続を許可する接続制御手段とを備えることとしてもよい。

又、本発明は、通信制御サーバとネットワークで接続された通信端末に用いる接続制御プログラムであって、前記接続制御プログラムは、前記通信制御サーバに、当該通信端末への接続が許可された通信端末の登録要求をする許可通信端末登録要求ステップと、前記通信端末のネットワーク上におけるアドレスを特定するための宛先情報を要求した通信端末が前記通信端末への接続が許可された通信端末である場合に限り、前記通信制御サーバから送信される、前記宛先情報を要求した通信端末を認証するための認証情報を受信する認証情報受信ステップと、前記宛先情報を要求した通信端末から、接続受入要求と当該通信端末を識別するための識別情報を受信する識別情報受信ステップと、前記認証情報と前記識別情報とが一致するか否かを判定する判定ステップと、前記認証情報と前記識別情報とが一致する場合に限り、前記宛先情報を要求した通信端末からの接続受入要求に基づく接続を許可する接続制御ステップとを含むこととしてもよい。

又、本発明は、通信制御サーバとネットワークで接続された通信端末に用いる接続制御プログラムを記録したコンピュータ読取可能な記録媒体であって、前記接続制御プログラムは、前記通信制御サーバに、当該通信端末への接続が許可された通信端末の登録要求をする許可通信端末登録要求ステップと、前記通信端末のネットワーク上におけるアドレスを特定するための宛先情報を要求した通信端末が前記通信端末への接続が許可された通信端末である場合に限り、前記通信制御サーバから送信

される、前記宛先情報を要求した通信端末を認証するための認証情報を  
受信する認証情報受信ステップと、前記宛先情報を要求した通信端末か  
ら、接続受入要求と当該通信端末を識別するための識別情報を受信する  
識別情報受信ステップと、前記認証情報と前記識別情報とが一致するか  
5 否かを判定する判定ステップと、前記認証情報と前記識別情報とが一致  
する場合に限り、前記宛先情報を要求した通信端末からの接続受入要求  
に基づく接続を許可する接続制御ステップとを含むこととしてもよい。

又、本発明は、通信制御サーバとネットワークで接続された通信端末  
に用いる接続制御方法であって、前記通信制御サーバに、当該通信端末  
10 への接続が許可された通信端末の登録要求をする許可通信端末登録要求  
ステップと、前記通信端末のネットワーク上におけるアドレスを特定す  
るための宛先情報を要求した通信端末が前記通信端末への接続が許可さ  
れた通信端末である場合に限り、前記通信制御サーバから送信される、  
前記宛先情報を要求した通信端末を認証するための認証情報を受信する  
15 認証情報受信ステップと、前記宛先情報を要求した通信端末から、接続  
受入要求と当該通信端末を識別するための識別情報を受信する識別情報  
受信ステップと、前記認証情報と前記識別情報とが一致するか否かを判  
定する判定ステップと、前記認証情報と前記識別情報とが一致する場合  
に限り、前記宛先情報を要求した通信端末からの接続受入要求に基づく  
20 接続を許可する接続制御ステップとを含むこととしてもよい。

これにより、接続を要求する通信端末に対する認証情報の発行作業を  
、通信制御サーバが代行することができるので、接続を要求された通信  
端末は、より簡易に認証作業を進めることができる。

ここで、前記通信システムにおいて、前記通知制御手段はさらに、第  
25 1 通信端末と第 2 通信端末間で送受信される情報を暗号化及び復号化す  
るための暗号鍵を作成する暗号鍵作成手段を有し、前記通知制御手段は  
さらに、前記暗号鍵を第 1 通信端末と第 2 通信端末に通知することとし  
てもよい。

これにより、通信端末間で送受信される認証情報が、第 3 者に不正に

取得され、解読されることを有効に防止することができる。

ここで、前記通信端末において、前記通信端末はさらに、接続先通信  
端末に送信すべき各種通信データを当該通信データのデータ属性と対応  
付けて記憶している記憶手段と、前記接続先通信端末のネットワーク上  
5 におけるアドレスを特定するための宛先情報を要求する要求メッセージ  
を前記通信制御サーバに送信する送信手段と、前記通信端末が前記接続  
先通信端末によって接続が許可された通信端末である場合に限り、前記  
通信制御サーバから通知される前記宛先情報を取得する取得手段と、取  
得された前記宛先情報に基づいて、前記接続先通信端末との接続を確立す  
10 る接続確立手段と、送信すべき通信データの指定を受取る指定受取手段  
と、指定された通信データが特定のデータ属性を有するか否か判定する  
データ属性判定手段と、指定された通信データが特定のデータ属性を有  
する場合に、前記通信制御サーバに、指定された通信データの前記接続  
先通信端末への転送を依頼する転送依頼手段と、指定された通信データ  
15 が特定のデータ属性を有する場合に、指定された通信データを前記通信  
制御サーバに送信し、指定された通信データが特定のデータ属性を有し  
ない場合に、指定された通信データを接続している前記接続先通信端末  
に直接送信する制御を行なう送信制御手段とを備えることとしてもよい。

又、前記通信端末において、前記アドレスは、IPアドレスであるこ  
20 ととしてもよい。

又、前記通信端末において、前記アドレスは、IPアドレスとポート  
番号とから構成されることとしてもよい。

又、前記通信端末において、前記アドレスは、随時変動することとし  
てもよい。

25 これにより、接続先通信端末に送信すべき通信データが特定の種類の  
属する場合に限り、通信制御サーバ経由で通信データが接続先通信端末  
に送信され、その他の場合には、通信データが直接接続先通信端末に送  
信されるように制御することができるので、通信制御サーバの通信デー  
タの送信に要する負荷を軽減することができる。



ここで、前記通信端末において、前記送信制御手段は、指定された通信データがMPEG符号化された映像データである場合に、当該映像データからIピクチャを抽出する抽出手段と、抽出したIピクチャを暗号化する暗号化手段とを有し、

- 5 前記転送依頼手段は、暗号化されたIピクチャの前記接続先通信端末への転送を依頼し、前記送信制御手段は、暗号化したIピクチャを前記通信制御サーバに送信し、Iピクチャを除く残りの映像データを接続している前記接続先通信端末に直接送信することとしてもよい。

- 10 これにより、映像データの再生に不可欠な構成要素であるIピクチャだけが通信制御サーバ経由で暗号化されて接続先通信端末に送信され、他の映像データの構成要素は、暗号化されることなく直接接続先通信端末に送信されるように制御することができるので、接続先通信端末における暗号化されたデータの復号化に要する負荷を軽減することができ、  
15 又、映像データの再生に不可欠なIピクチャは、暗号化されて送信されるので、送信途中で映像データが何者かによって不正に取得された場合においても取得された映像データが不正に再生されて視聴されるのを防止することができる。

- ここで、前記通信端末において、前記データ属性は、通信データの秘匿性の有無を示すデータ属性であり、前記転送依頼手段は、指定された  
20 通信データのデータ属性が秘匿性の有ることを示している場合に、前記通信制御サーバに、指定された通信データの前記接続先通信端末への転送を依頼し、前記送信制御手段は、指定された通信データのデータ属性が秘匿性の有ることを示している場合に、指定された通信データを暗号化して前記通信制御サーバに送信することとしてもよい。

- 25 これにより、秘匿性の高いデータは、通信制御サーバを介して暗号化されて接続先通信端末に送信され、秘匿性の低いデータのみが直接接続先通信端末に送信されるように制御することができるので、ユーザーは予め通信端末に記録しているデータを秘匿性の程度に応じて分類して記録することにより、秘匿性の高いデータが不正に取得され、他人に視聴

されるといふ心配なく、安心して接続先通信端末にデータを送信することができる。

ここで、前記通信システムにおいて、前記通知制御手段はさらに、第2通信端末の宛先情報を第1通信端末に通知する前に、第2通信端末が第1通信端末からの接続を受入可能か否かについての問合せメッセージを第2通信端末に送信し、  
第2通信端末は、前記問合せメッセージを受信する受信手段と、前記問合せメッセージの受信時における負荷状態に応じて、第1通信端末からの接続の受入可否を判定し、判定結果を示す受入可否通知メッセージを前記通信制御サーバに通知する接続受入可否通知手段とを有し、前記通知制御手段は、通知された受入可否通知メッセージに基づいて、第2通信端末が、第1通信端末からの接続を受入可能な状態にあるか否かを判定する接続受入可否判定手段を有し、第2通信端末が、第1通信端末からの接続を受入可能な状態にある場合に限り、前記通知制御手段は、第2通信端末の宛先情報を第1通信端末に通知することとしてもよい。

又、前記通信端末において、前記識別情報受信手段はさらに、前記接続受入要求が送信される前に、前記宛先情報を要求した通信端末からの接続を受入可能か否かについての問合せメッセージを、前記通信制御サーバから受信し、前記接続制御手段は、前記問合せメッセージの受信時における負荷状態に応じて、前記接続が受入可能か否かを判定し、判定結果を前記通信制御サーバに通知することとしてもよい。

これにより、利用者の通信端末の負荷状態に応じて、他の通信端末からの接続が制御されるので、負荷が高い状態のときに、他の通信端末からの接続が受けられ、通信に不具合が生じるのを有効に防止することができる。

ここで、前記通信システムにおいて、前記通知制御手段は、第1通信端末が第2通信端末に接続を許可されている通信端末でない場合に、その旨を示す第1通知メッセージを第1通信端末に通知し、第2通信端末が、第1通信端末からの接続を受入可能な状態にない場合に、その旨を

示す第2通知メッセージを第1通信端末に通知することとしてもよい。

これにより、接続要求元の通信端末が接続要求先の通信端末への接続ができなかった場合に、その原因が特定されて接続要求元の通信端末に通知されるので、ユーザーは、迅速に接続ができない原因を知ることができる。

ここで、前記通信端末において、前記識別情報受信手段は、前記宛先情報を要求した通信端末からの接続を受入可能な状態にない場合に、前記通信制御サーバから、宛先情報を要求した通信端末からの通信データの転送依頼があったことを通知する転送依頼通知メッセージを受信し、  
10 前記通信端末は、負荷状態に応じて前記通信データを取得可能な状態になったか否かを判定する通信データ取得可否判定手段と、前記転送依頼通知メッセージが受信された後に、前記通信データを取得可能な状態になった場合に、前記通信データの転送を要求する転送要求メッセージを前記通信制御サーバに送信する転送要求メッセージ送信手段と、前記転送要求メッセージに応じて前記通信制御サーバから送信された前記通信データを取得する取得手段とを備えることとしてもよい。

これにより、接続先通信端末が接続受入状態になく、通信データを直接送信できない場合に、通信制御サーバに通信データの転送を依頼することができるので、何度も接続先通信端末との接続確立処理を繰り返すことなく、迅速に通信データの送信処理を完了することができる。

#### 図面の簡単な説明

図1は、本発明の実施の形態1における通信システム100の構成を示す機能ブロック図である。

25 図2は、仲介サーバ101の構成を示す機能ブロック図である。

図3は、仲介サーバ101に送信される許可端末登録コマンドの具体例を示す。

図4は、許可端末テーブルの具体例を示す。

図5(a)は、問合せメッセージの具体例を示す。

- 図 5 (b) は、「接続受入」を示す通知メッセージの例を示す。
- 図 5 (c) は、「接続拒否」を示す通知メッセージの例を示す。
- 図 5 (d) は、接続先通知メッセージの具体例を示す。
- 図 5 (e) は、認証情報通知メッセージの具体例を示す。
- 5 図 5 (f) は、接続受入要求メッセージの具体例を示す。
- 図 5 (g) は、図 1 2 及び図 1 6 のステップ S 1 2 0 5 における判定が否定的である場合に送信される通知メッセージの変形例を示す。
- 図 5 (h) は、図 1 6 のステップ S 1 6 0 8 における判定が否定的である場合に送信される通知メッセージの変形例を示す。
- 10 図 6 は、アドレス解決サーバ 1 0 2 の構成を示す機能ブロック図である。
- 図 7 は、IP アドレス対応テーブルの具体例を示す。
- 図 8 は、仲介サーバ 1 0 1 から取得要求データを受信した後に、アドレス解決サーバ 1 0 2 の行う IP アドレス送信処理の動作を示すフロー
- 15 チャートである。
- 図 9 は、各端末の行う接続許可端末の登録要求処理の動作を示すフローチャートである。
- 図 1 0 は、仲介サーバ 1 0 1 による許可端末テーブルへの接続許可端末の登録処理 (図 9 のステップ S 1 0 0 0) の動作を示すフローチャ
- 20 トである。
- 図 1 1 は、各端末の行う他端末との接続確立処理の動作を示すフローチャートである。
- 図 1 2 は、図 1 1 のステップ S 1 1 0 1 において、送信された問合せメッセージを受信した仲介サーバ 1 0 1 が行う接続制御処理の動作を示
- 25 すフローチャートである。
- 図 1 3 は、図 1 1 のステップ S 1 1 0 7 において、端末 1 0 3 によって接続受入要求された端末 1 0 4 が行う他端末からの接続受入処理の動作を示すフローチャートである。

図 1 4 は、本発明の実施の形態 2 における通信システム 1 1 0 の構成

を示す機能ブロック図である。

図 15 は、仲介サーバ 111 の構成を示す機能ブロック図である。

図 16 は、制御部 211 の行う接続制御処理の動作を示すフローチャートである。

- 5 図 17 (a) は、図 16 のステップ S1606 において送信される、端末 114 に送信される受入状態問合せメッセージの具体例を示す。

図 17 (b) は、「接続受入状態にある」ことを示す、端末 114 から受信する返答通知メッセージの具体例を示す。

- 10 図 17 (c) は、「接続拒否状態にある」ことを示す、端末 114 から受信する返答通知メッセージの具体例を示す。

図 18 は、端末 114 が、図 13 に示す接続受入処理と同一の処理を行う前に実行する接続受入状態の通知処理の動作を示すフローチャートである。

- 15 図 19 は、仲介サーバ 111 の行なう接続確立判定処理の動作を示すフローチャートである。

図 20 は、端末 103 及び端末 104 の構成を示す機能ブロック図である。

図 21 は、通信システム 200 の構成を示す。

- 20 図 22 は、仲介サーバ 101 による端末間の通信データの転送処理の動作を示すフローチャートである。

図 23 は、各端末の行なう通信データ送信制御処理の動作を示すフローチャートである。

図 24 は、実施の形態 3 における通信システム 120 の構成を示す機能ブロック図である。

- 25 図 25 は、仲介サーバ 121 の構成を示す機能ブロック図である。

図 26 及び図 27 は、制御部 221 の行う接続制御処理の動作を示すフローチャートである。

図 28 は、仲介サーバ 121 によるステップ S2611 による処理を介して送信された転送依頼問合せメッセージを端末 123 が受信した場

合に、端末 1 2 3 が行なう通信データ転送依頼処理の動作を示すフローチャートである。

図 2 9 は、仲介サーバ 1 2 1 による図 2 7 のステップ S 2 6 1 5 による処理を介して送信された転送依頼通知メッセージを端末 1 2 4 が受信した場合に、端末 1 2 4 が行なう通信データ受入制御処理の動作を示すフローチャートである。

図 3 0 は、端末 1 1 4 の構成を示す機能ブロック図である。

図 3 1 は、端末 1 2 3 の構成を示す機能ブロック図である。

図 3 2 は、端末 1 2 4 の構成を示す機能ブロック図である。

10

発明を実施するための最良の形態

(実施の形態 1)

<構成>

図 1 は、本発明の実施の形態 1 における通信システム 1 0 0 の構成を示す機能ブロック図である。通信システム 1 0 0 は、仲介サーバ 1 0 1、アドレス解決サーバ 1 0 2、通信端末 1 0 3 (以下、「端末 1 0 3」という。)、通信端末 1 0 4 (以下、「端末 1 0 4」という。) とから構成され、各構成要素はインターネット 1 0 5 で接続されている。

なお、仲介サーバ 1 0 1 とアドレス解決サーバ 1 0 2 はインターネットを介した接続ではなく、同じイントラネット (例えば、LAN) に接続されている構成であっても良い。

又、ここでは、説明を簡略化するため、通信システム 1 0 0 の構成要素となる通信端末 (以下、「端末」という。) の数は 2 としたが、端末の数は複数であればよく、2 に限定されない。

又、端末とは、インターネットやイントラネットに接続機能を有する機器のことをいい、具体的には PC (Personal Computer)、HDD (Hard Disk Drive) ビデオレコーダ、DVD レコーダ、TV (Television)、PDA (Personal Digital Assistance) などのことをいう。

図 2 1 は、通信システム 1 0 0 を構成する各端末が HDD ビデオレコ

- ーダである場合の通信システム 200 の具体例を示す。なお、図 21 では、通信システム 100 の構成を簡略化して図示するため、アドレス解決サーバは、図示していない。通信システム 200 は、接続要求元の端末である HDD ビデオレコーダ 1030、接続先の端末である HDD ビデオレコーダ 1040、仲介サーバ 1010 から構成される。

図 2 は、仲介サーバ 101 の構成を示す機能ブロック図である。

- 仲介サーバ 101 は、制御部 201、送信部 202、受信部 203、パスワード発行部 204、暗号鍵発行部 205、記憶部 206 から構成される。
- 10 仲介サーバ 101 は、ハードウェアとしては CPU、ROM、RAM、ハードディスク等から構成され、ROM 又は上記ハードディスクには、コンピュータプログラムが記憶され、上記 CPU が、上記コンピュータプログラムに従って動作することにより、仲介サーバ 101 は、その機能を達成する。
- 15 受信部 203 は、各端末から送信された、接続先の端末（以下、「接続先端末」という。）の IP アドレスを、当該端末の識別子を特定して問い合わせるメッセージ（以下、「問合せメッセージ」という。）を受信し、制御手段 201 へ出力する。図 5（a）は、問合せメッセージの具体例を示す。
- 20 ここで、「QUERY」は、問合せメッセージであることを示し、「Identifier」は、問合せメッセージの送信元の端末（以下、「問合せ端末」という。）の識別子を示し、「Callee」は、接続先端末の識別子を示す。
- 又、受信部 203 は、各端末から送信された登録要求データを受信し、制御部 201 へ出力する。
- 25 ここで、「登録要求データ」とは、各端末によって作成される、当該端末への接続を許可された端末（以下、「接続許可端末」という。）の登録や登録された接続許可端末の削除を要求する許可端末登録コマンドと仲介サーバ 101 の IP アドレスとを含むパケット化データのことをいう。

ここで、許可端末登録コマンドには、登録を要求した端末の識別子と、当該端末によって登録や削除を要求される接続許可端末の識別子と、登録処理の内容を示すコマンドが含まれる。

図3は、仲介サーバ101に送信される許可端末登録コマンドの具体例を示す。図3(a)は、新たに登録を行う場合のコマンドメッセージの一例を示す。「REGISTER」は登録処理を表すコマンドを示し、「Identifier」は、接続許可の主体となる各端末の識別子を示し、「Accept」は、仲介サーバ101における登録処理で行うべき具体的な処理の内容を、それに続く命令文(ここでは、「Create」を含む命令文)で指示するコマンドを示し、「Create」は新たに接続許可端末を登録するコマンドを表し、ここでは、「Create」を含む命令文は、接続許可端末として既に登録されている接続許可端末の識別子を削除して、識別子Ib、Ifの接続許可端末を新たに登録するコマンドを表している。

図3(b)の「Add」は、既に登録されている接続許可端末の識別子に加え、新たに接続許可端末の識別子を追加するコマンドを表している。ここでは、「Add」を含む命令文は、識別子Ic、Ieの端末を、接続許可端末として追加して登録するコマンドを表している。

図3(c)の「Delete」は、既に登録されている接続許可端末の識別子から指定の識別子を取り除き、接続許可を取り消すコマンドを表している。ここでは、「Delete」を含む命令文は、既に登録されている接続許可端末の識別子から、識別子Ifを削除するコマンドを表している。なお、図3(b)の「Add」と図3(c)の「Delete」のコマンドは図3(d)に示すようにひとつのコマンドとしても良い。

送信部202は、制御部201から入力された、認証情報通知メッセージを接続先端末に送信する。

ここで、「認証情報通知メッセージ」とは、接続受入を要求された端末が、問合せ端末を認証するために用いる情報を含むメッセージのことをいい、具体的には、制御部201によって作成される、問合せ端末の識別子、当該端末を認証するためのパスワード、及び当該端末との通信



データを暗号化及び復号化するための暗号鍵を含むメッセージのことをいう。

ここで、「通信データ」とは、端末間で送受信される映像データ、画像データ、音声データ、テキストデータなどの各種データのことをいう。

5 図5(e)は、認証情報通知メッセージの具体例を示す。

ここで、「NOTIFY」は、通知メッセージであることを示し、「Caller ID」は、問合せ端末の識別子を示し、「Password」は、上記パスワードを、「Encrypt Key」は、上記暗号鍵を示す。

10 又、送信部202は、制御部201から入力された、接続先通知メッセージを問合せ端末に送信する。

ここで、「接続先通知メッセージ」とは、問合せ端末に接続先の端末のIPアドレスを通知するために用いるメッセージのことをいい、具体的には、制御部201によって作成される、当該問合せ端末に問い合わせられた接続先端末のIPアドレスと、当該問合せ端末を認証するためのパスワードと、当該接続先端末との通信データを暗号化及び復号化するための暗号鍵とを含むメッセージのことをいう。

図5(d)は、接続先通知メッセージの具体例を示す。

ここで、「NOTIFY」は、通知メッセージであることを示し、「Callee Address」は、接続先端末のIPアドレスを示し、「Password」は、上記パスワードを、「Encrypt Key」は、上記暗号鍵を示す。

20 さらに、送信部202は、制御部201から入力された、接続先端末の識別子を特定してIPアドレスの取得要求をする取得要求コマンドと仲介サーバ101のIPアドレスとアドレス解決サーバ102のIPアドレスとを含むパケット化データ（以下、「取得要求データ」という。）をアドレス解決サーバ102に送信する。

25 パスワード発行部204は、制御部201からのパスワード発行指示に基づいて、パスワードとなる文字列を発行する。

ここで、パスワードとして発行される文字列は、例えば、アルファベット大文字小文字、数字、記号又はそれらが複数混在したものであり、

毎回異なる文字列が発行される。例えば、アルファベット大文字小文字、数字や記号などをランダムに組み合わせた、複数の文字列のリストから、パスワードとなる文字列が任意に選択されて、発行されるものとしてもよい。

- 5 暗号鍵発行部 205 は、制御部 201 からの暗号鍵発行指示により、データの暗号化及び復号化に用いる暗号鍵を発行するものである。

ここでは、送信するデータの暗号化と、当該暗号化データの受信側における復号化を同一の暗号鍵を用いて行う共通鍵方式の暗号鍵を発行するものとする。

- 10 記憶部 206 は、ハードディスクやフラッシュメモリなどによって構成され、許可端末テーブル、許容通信データサイズ閾値、上記コンピュータプログラム、アドレス解決サーバ 102 のアドレスなどを記憶している。

- 15 ここで、「許可端末テーブル」とは、各端末からの登録要求に応じて、制御部 201 によって登録された、当該端末と当該端末の接続許可端末との対応関係を示すテーブルのことをいう。

又、「許容通信データサイズ閾値」とは、後述する通信データの転送処理において、端末から送信される通信データを受け入れるか否かを判定するための通信データの許容データサイズの閾値のことをいう。

- 20 又、「アドレス」とは、例えば、URL (Uniform Resource Locator)、或いは IP アドレスなどのことをいう。

- 図 4 は、許可端末テーブルの具体例を示す。図 3 に示す例では、識別子が Ia の端末に対しては、識別子が Ib、Ic、及び Ie の各端末からの接続が許可され、識別子が Ib の端末に対しては、識別子が Ia、Ic、If、及び Ig の各端末からの接続が許可されていることを示す。

- 25 制御部 201 は、記憶部 206 に記憶されているコンピュータプログラムを読み出して実行することにより、他の各構成要素の動作を制御するとともに、許可端末テーブルへの接続許可端末の登録処理、端末間の接続を制御する接続制御処理、及び端末間の通信データの転送処理を行

う。

以下制御部 201 の行う上記 3 つの処理について、具体的に説明する。

(1) 許可端末テーブルへの接続許可端末の登録処理

- 5 制御部 201 は、受信部 202 から登録要求データの入力があると、登録要求データから許可端末登録コマンドを抽出し、抽出した許可端末登録コマンドの内容を解析し、「REGISTER」コマンドを検出すると、上記登録処理の実行が指示されていることを認識し、許可端末登録コマンドの指示する処理内容（Acceptに続く命令文で指示するコマンド）を実行
- 10 する。

- 具体的には、処理内容が「Create」を含む命令文で示されている場合には、許可端末テーブルを参照して、登録を要求した端末が既に登録されているか否かを判定し、登録されていない場合には、当該端末の識別子と当該端末によって登録要求された接続許可端末の識別子を対応づけて、許可端末テーブルに新たに登録し、登録されている場合には、当該
- 15 端末について、登録済みの接続許可端末の識別子を許可端末テーブルから削除した後、登録要求された接続許可端末の識別子を許可端末テーブルに新たに登録する。

- 処理内容が「Add」を含む命令文で示されている場合には、登録を要求した端末について、許可端末テーブルに登録済みの接続許可端末の識別子が有る場合においても、当該接続許可端末を削除することなく、登録要求された接続許可端末の識別子を許可端末テーブルに追加登録する。

- 処理内容が「Delete」を含む命令文で示されている場合には、削除要求された接続許可端末の識別子を許可端末テーブルから削除する。
- 25

上記各処理内容の実行が終了すると、登録処理の成否を示す登録結果メッセージを作成し、登録要求した端末に送信部 202 を介して送信する。例えば、登録処理が成功した場合には、「登録完了」を示すメッセージ（以下、「登録完了メッセージ」という。）を作成し、登録処理が失敗

した場合には、「登録失敗」を示すメッセージ（以下、「登録失敗メッセージ」という。）を作成する。又、処理のステータスコードで、「登録完了」及び「登録失敗」を表したメッセージを作成することとしてもよいし、文字列と処理のステータスコードの両方でメッセージを作成することとしてもよい。

## （２）接続制御処理

制御部 201 は、受信部 203 より問合せメッセージの入力を受取ると、記憶部 206 に記憶されている許可端末テーブルを参照することにより、問合せメッセージによって特定されている接続先端末の識別子により、問合せメッセージによって特定されている接続先端末の識別子と対応付けられている接続許可端末の識別子を特定し、特定した識別子と問合せ端末の識別子が一致するか否かにより、問合せ端末が、接続先端末への接続が許可されている端末に該当するか否かを判定し、判定結果を通知する通知メッセージを問合せ端末に送信する。

図 5（b）と図 5（c）は、当該問合せ端末に送信される通知メッセージの具体例を示す。図 5（b）は、「接続受入」を示す通知メッセージの例を示し、図 5（c）は、「接続拒否」を示す通知メッセージの例を示している。

問合せ端末が、接続先端末への接続が許可されている端末に該当する場合には、取得要求データを、送信部 202 を介してアドレス解決サーバ 102 に送信し、接続先端末の IP アドレスをアドレス解決サーバ 102 から取得すると、「接続受入」を示す通知メッセージを問合せ端末に送信する。

次に、制御部 201 は、パスワード発行部 204 にパスワード発行指示を、暗号鍵発行部 205 に暗号鍵発行指示をし、指示に応じてパスワード発行部 204 及び暗号鍵発行部 205 からそれぞれ発行されたパスワード及び暗号鍵と、問合せ端末の識別子とから、認証情報通知メッセージを作成し、作成した認証情報通知メッセージを、通信部 202 を介して接続先端末に送信する。

次に、制御部 201 は、発行されたパスワードと暗号鍵、及び取得し

た接続先端末のIPアドレスとから、接続先通知メッセージを作成し、送信部202を介して問合せ端末に送信する。

又、問合せ端末が、接続先端末への接続が許可されている端末に該当しない場合には、「接続拒否」を示す通知メッセージを問合せ端末に送信する。

### (3) 端末間の通信データの転送処理

制御部201は、受信部203より通信データ転送通知メッセージを受取ると、当該通信データ依頼メッセージに含まれる通信データのデータサイズ情報に基づいて、通信データのデータサイズが許容通信データサイズ閾値を超えているか否かを判定し、超えていない場合に、「通信データの受入を許可する」旨の転送受入通知メッセージを作成して、送信部202を介して転送受入通知メッセージを転送依頼元の端末に送信し、当該転送受入通知メッセージに応じて当該端末より送信された暗号化通信データを受信部203を介して受取ると、送信部202を介して接続先端末に送信する。

ここで、「通信データ転送通知メッセージ」とは、送信元端末から接続先端末に送信すべき通信データが秘匿性の高い秘匿データである場合に、当該データの送信を仲介サーバ101に依頼するために送信元端末（ここでは、問合せ端末）から仲介サーバ101に送信されるメッセージのことをいい、具体的には、問合せ端末の識別子と接続先端末の識別子と通信データのデータサイズ情報と仲介サーバ101のIPアドレスとを含むメッセージのことをいう。

又、「転送受入通知メッセージ」とは、通信データの送信元の端末から受入要求された場合に、仲介サーバ101又は接続先端末から送信元の端末に通知される、通信データの受け入れを許可するか否かを示すメッセージのことをいい、具体的には、通知メッセージであることを示す識別子と通知内容と通知元の識別子と送信元の端末のIPアドレスとを含むメッセージのことをいう。

次にアドレス解決サーバ102について説明する。図6は、アドレス

解決サーバ１０２の構成を示す機能ブロック図である。

アドレス解決サーバ１０２は、制御部３０１、送信部３０２、受信部３０３、記憶部３０４から構成される。

５ アドレス解決サーバ１０２は、ハードウェアとしてはＣＰＵ、ＲＯＭ、ＲＡＭ、ハードディスク等から構成され、ＲＯＭ又は上記ハードディスクには、コンピュータプログラムが記憶され、上記ＣＰＵが、上記コンピュータプログラムに従って動作することにより、アドレス解決サーバ１０２は、その機能を達成する。

１０ 送信部３０２は、制御部３０１より入力された、接続先端末のＩＰアドレスと仲介サーバ１０１のＩＰアドレスとを含むパケット化データ（以下、「接続先ＩＰアドレスデータ」という。）を、仲介サーバ１０１に送信する。

１５ 受信部３０３は、仲介サーバ１０１から送信された取得要求データ、及びインターネットに接続している各端末から送信された、当該端末のＩＰアドレス及び識別子とアドレス解決サーバ１０２のＩＰアドレスとを含むパケット化データ（以下、「接続端末ＩＰアドレスデータ」という。）を受信し、制御部３０１に出力する。

２０ 記憶部３０４は、ハードディスクやフラッシュメモリなどによって構成され、ＩＰアドレス対応テーブルや、制御部３０１が実行するプログラムなどを記憶している。

ここで、「ＩＰアドレス対応テーブル」とは、インターネットに接続されている端末と当該端末に割当てられたＩＰアドレスとの対応関係を示すテーブルのことをいう。

２５ 図７は、ＩＰアドレス対応テーブルの具体例を示す。図７の例では、識別子がＩａ及びＩｂの端末がそれぞれ、インターネットに接続され、識別子がＩａの端末には、ＩＰアドレス（２０２．２２４．１８６．８１）が、識別子がＩｂの端末には、ＩＰアドレス（２０２．２２４．１８６．８２）が、それぞれ割当てられていることを示す。

制御部３０１は、受信部３０３より接続端末ＩＰアドレスデータの入

力があると、当該IPアドレスデータから当該端末のIPアドレス及び識別子を抽出し、抽出したIPアドレスと識別子を対応付けて、IPアドレス対応テーブルに登録する。

又、制御部301は、受信部303より取得要求データの入力がある  
5 と、当該取得要求データから接続先端末の識別子を抽出し、記憶部304に記憶されているIPアドレス対応テーブルを参照して、当該識別子に対応するIPアドレスを特定し、当該IPアドレスと仲介サーバ101のIPアドレスとから接続先IPアドレスデータを作成し、作成した接続先IPアドレスデータを、送信部302を介して仲介サーバ101  
10 に送信する。

次に、端末103及び端末104について説明する。両端末の構成は、同一であり、図20は、その構成を示す機能ブロック図である。両端末は、それぞれ、制御部401、送信部402、受信部403、暗号化部404、復号化部405、記憶部406、入力部407から構成され  
15 る。

又、両端末は、ハードウェアとしては、CPU、ROM、RAM、ハードディスク等から構成され、ROM又は上記ハードディスクには、コンピュータプログラムが記憶され、上記CPUが、上記コンピュータプログラムに従って動作することにより、両端末は、その機能を達成する  
20 。

各端末は、あらかじめ、仲介サーバ101及びアドレス解決サーバ102のアドレス、映像データ、画像データ、音声データ、テキストデータなどの各種通信データ、及び通信データ秘匿性判定テーブルなどを記憶部406に記憶している。

25 ここで、「通信データ秘匿性判定テーブル」とは、各通信データと当該通信データが秘匿性のものであるか否かを示す秘匿性判定識別子との対応関係を示すテーブルのことをいう。

なお、通信データが秘匿性のものであるか否かは、例えば当該通信データの記録時に、入力部407を介してユーザーによって指示され、制

御部 401 は、ユーザー指示に応じて、通信データ秘匿性テーブルにおいて、当該通信データの秘匿性判定識別子を設定するものとする。

各端末は、インターネットに接続すると、プロバイダーのサーバ（図外）から割当てられた、IPアドレスと当該端末の識別子とを、送信部 402 を介して、アドレス解決サーバ 102 に送信する。

さらに、各端末は、接続許可端末の登録要求処理、他端末との接続確立処理、他端末からの接続受入処理、他端末との接続確立後における通信データ送信制御処理を行う。以下、各処理について、具体的に説明する。

#### 10 (1) 接続許可端末の登録要求処理

制御部 401 は、ユーザーによって入力部 407 から入力された、登録を要求する接続許可端末の識別子と、仲介サーバ 101 の IP アドレスに基づいて登録要求データを作成し、作成した登録要求データを仲介サーバ 101 に送信し、仲介サーバ 101 から、当該接続許可端末の許可  
15 可端末テーブルへの登録処理の成否を示す登録結果メッセージを受信部 403 を介して受信すると、処理を終了する。

#### (2) 他端末との接続確立処理

制御部 401 は、ユーザーから、入力部 407 を介して接続先となる端末の IP アドレスの問合せ指示の入力があると、仲介サーバ 101 に  
20 、問合せメッセージを送信部 402 を介して送信し、仲介サーバ 101 から送信された通知メッセージを受信部 403 を介して受信する。

当該通知メッセージが「接続拒否」を示している場合、制御部 401 は、処理を終了し、「接続受入」を示している場合、さらに、仲介サーバ 101 から、接続先通知メッセージを受信部 403 を介して受信する。

25 次に、制御部 401 は、受信部 403 を介して受信した接続先通知メッセージに含まれるパスワードと当該端末の識別子とを用いて、接続受入要求メッセージを作成し、暗号化部 404 を介して、作成した接続受入要求メッセージを、受信した接続先通知メッセージに含まれる暗号鍵を用いて暗号化し、暗号化した接続受入要求メッセージを、送信部 40



2を介して接続先端末に送信して当該接続先端末に対し、接続受入要求をする。

図5(f)は、接続受入要求メッセージの具体例を示す。「REQUEST」は、接続受入要求メッセージであることを示し、「Identifier」は、要求  
5 元の端末の識別子を示し、「Password」は、当該接続受入メッセージに記述されているパスワードを示す。

さらに、制御部401は、当該接続先端末から受入可否の判定結果を示す通知メッセージを、受信部403を介して受信すると、当該通知メッセージの内容を解釈し、接続受入の可否を判定する。

10 通知メッセージが「接続拒否」を示す場合、制御部401は、処理を終了し、「接続受入」を示す場合、接続先端末とのデータ通信を開始し、後述する通信データ送信制御処理を行なう。

### (3) 他端末からの接続受入処理

制御部401は、仲介サーバ101から、認証情報通知メッセージを  
15 、受信部403を介して受信すると、当該認証情報通知メッセージから問合せ端末の識別子、パスワード及び暗号鍵を取得する。

さらに、制御部401は、他端末から、接続受入要求メッセージを、受信部403を介して受取ると、当該接続受入要求メッセージを取得した暗号鍵を用いて、復号化部405を介して復号し、当該接続受入要求  
20 メッセージから、当該他端末の識別子とパスワードを取得し、取得した識別子、パスワードについてそれぞれ、先に認証情報通知メッセージから取得した識別子、パスワードとの照合を行う。

識別子とパスワードの何れもが一致する場合、制御部401は、「接続受入」を示す通知メッセージを作成し、取得した暗号鍵を用いて、暗  
25 号化部404を介して暗号化して、接続受入要求をした他端末に、送信部402を介して送信し、他端末とのデータ通信を開始する。

識別子とパスワードの何れかが一致しない場合、制御部401は、「接続拒否」を示す通知メッセージを作成し、取得した暗号鍵を用いて、暗号化部404を介して暗号化して、接続受入要求をした他端末に、送

信部 402 を介して送信し、当該他端末との接続を中止する。

#### (4) 通信データ送信制御処理

制御部 401 は、入力部 407 を介して、ユーザーから接続先端末に送信すべき通信データの指定を受取ると、当該通信データを記憶部 406 から読出し、記憶部 406 に記憶されている通信データ秘匿性判定  
5 テーブルを参照して、指定された通信データが秘匿性データであるか否かを判定し、秘匿性データである場合、通信データ転送通知メッセージを作成して、仲介サーバ 101 及び接続先端末に送信し、仲介サーバ 101 及び接続先端末から「通信データの受入を許可する」旨の転送受入  
10 通知メッセージを受信部 403 を介して受取ると、指定された通信データを、受信部 403 を介して受信した接続先通知メッセージに含まれる暗号鍵を用いて暗号化して、送信部 402 を介して仲介サーバ 101 に送信する。

指定された通信データが秘匿性データでない場合、制御部 401 は、  
15 読出した通信データを暗号化することなく、接続先端末に直接送信する。

これにより、例えば、図 21 に示す通信システム 200 を用いて、HDD ビデオレコーダに記録した「運動会の映像データ」を、仲介サーバ 101 を介して暗号化して親戚や祖父母宅にある HDD ビデオレコーダ  
20 にインターネット経由で送信することができるので、送信した映像データを途中で他人に解読されるという危険性がなく、記録した映像を遠隔地に居住する親戚や祖父母と一緒に楽しむことができる。

又、TV 番組の録画データなど他人に見られても特に支障のない通信データの場合には、仲介サーバ 101 を介することなく、直接接続先の  
25 HDD ビデオレコーダに通信データを送信して、録画した TV 番組と一緒に楽しむことができる。

#### <動作>

最初に、仲介サーバ 101 から取得要求データを受信した後に、アドレス解決サーバ 102 の行う IP アドレス送信処理の動作について説明

する。

図 8 は、上記動作を示すフローチャートである。以下、図 8 を参照して、上記動作について説明する。

受信部 303 は、仲介サーバ 101 から取得要求データを受信すると  
5 (ステップ S801)、受信した取得要求データを制御部 301 に出力する。

制御部 301 は、受信部 303 より取得要求データの入力があると、  
当該取得要求データから接続先端末の識別子を抽出し (ステップ S802)、記憶部 304 に記憶されている IP アドレステーブルを参照して、  
10 当該識別子が IP アドレステーブルに登録されているか否かを判定する (ステップ S803)。

登録されている場合 (ステップ S803 : Y)、当該識別子に対応する IP アドレスを IP アドレステーブルから特定し (ステップ S804)、当該 IP アドレスと仲介サーバ 101 の IP アドレスとから接続先 IP  
15 アドレスデータを作成し (ステップ S805)、作成した接続先 IP アドレスデータを、送信部 302 を介して仲介サーバ 101 に送信する (ステップ S806)。

登録されていない場合 (ステップ S803 : N)、「未登録」である旨を示すメッセージ (以下、「未登録メッセージ」という。) を作成して、  
20 送信部 302 を介して仲介サーバ 101 に送信する (ステップ S807)。

次に、各端末の行う接続許可端末の登録要求処理の動作について説明する。図 9 は、上記動作を示すフローチャートである。以下、図 9 を参照して上記動作について説明する。

25 なお、ここでは、説明を簡略化するため、端末 104 が端末 103 を接続許可端末として登録を要求するものとして、上記動作について説明する。

端末 104 は、登録要求データを作成し (ステップ S901)、作成した登録要求データを仲介サーバ 101 に送信し (ステップ S902)

、仲介サーバ１０１による許可端末テーブルへの接続許可端末（ここでは、端末１０３）の登録処理を開始させ（ステップＳ１０００）、当該登録処理が終了すると、仲介サーバ１０１から登録結果メッセージを受信する（ステップＳ９０３）。

- ５ 次に仲介サーバ１０１による許可端末テーブルへの接続許可端末の登録処理（ステップＳ１０００）の動作について説明する。

図１０は、上記動作を示すフローチャートである。以下、図１０を参照して説明する。

- 受信部２０３は、端末１０４から登録要求データを受信すると（ステップＳ１００１）、受信した登録要求データを制御部２０１に出力する。

- 制御部２０１は、受信部２０３から登録要求データの入力があると、登録要求データから許可端末登録コマンドを抽出し（ステップＳ１００２）、抽出した許可端末登録コマンドの内容を解析し（ステップＳ１００３）、上記登録処理の実行が指示されていることを認識すると、許可端末登録コマンドの指示する処理内容を実行し（ステップＳ１００４）、当該処理内容の実行に成功したか否かを判定する（ステップＳ１００５）。

- 成功した場合（ステップＳ１００５：Ｙ）、登録完了メッセージを作成し、送信部２０２を介して端末１０４に送信し（ステップＳ１００６）、失敗した場合（ステップＳ１００５：Ｎ）、登録失敗メッセージを作成し、送信部２０２を介して端末１０４に送信する（ステップＳ１００７）。

次に、各端末の行う他端末との接続確立処理の動作について説明する。図１１は、上記動作を示すフローチャートである。以下、図１１を参照して、上記動作について説明する。

- ２５ なお、ここでは、説明を簡略化するため、端末１０３が端末１０４との接続を確立する場合の上記動作について説明する。

端末１０３は、仲介サーバ１０１に、端末１０４の宛先を問合せするための問合せメッセージを送信する（ステップＳ１１０１）。

端末１０３は、当該問合せメッセージの返答として、仲介サーバ１０

1 から通知メッセージを受取ると(ステップS 1 1 0 2)、当該通知メッセージの内容を解析して(ステップS 1 1 0 3)、当該通知メッセージが「接続受入」を示しているか否かを判定する(ステップ1 1 0 4)。

5 端末1 0 3は、当該通知メッセージが「接続拒否」を示している場合(ステップS 1 1 0 4 : N)、処理を終了し、「接続受入」を示している場合(ステップS 1 1 0 4 : Y)、さらに、仲介サーバ1 0 1から、接続先通知メッセージを受信し(ステップS 1 1 0 5)、受信した接続先通知メッセージに含まれるパスワードと端末1 0 3の識別子とを用いて、接続受入要求メッセージを作成し(ステップS 1 1 0 6)、作成した接続受入要求メッセージを、受信した接続先通知メッセージに含まれる暗号鍵を用いて暗号化し、暗号化した接続受入要求メッセージを端末1 0 4に送信して端末1 0 4に対し、接続受入要求をし(ステップS 1 1 0 7)、端末1 0 4から受入可否の判定結果を示す通知メッセージを受信すると(ステップS 1 1 0 8)、当該通知メッセージの内容を解析し、接続受入の可否を判定する(ステップS 1 1 0 9)。

15 端末1 0 3は、通知メッセージが「接続拒否」を示す場合(ステップS 1 1 0 9 : N)、処理を終了し、「接続受入」を示す場合(ステップS 1 1 0 9 : Y)、端末1 0 4とのデータ通信を開始する(ステップS 1 1 1 0)。

20 次に、上記のステップS 1 1 0 1において、送信された問合せメッセージを受信した仲介サーバ1 0 1が行う接続制御処理の動作について説明する。図1 2は、上記動作を示すフローチャートである。以下、図1 2を参照して、上記動作について説明する。

25 受信部2 0 3は、端末1 0 3から送信された問合せメッセージを受信すると(ステップS 1 2 0 1)、当該問合せメッセージを制御部2 0 1に出力する。

制御部2 0 1は、受信部2 0 3より問合せメッセージの入力を受取ると、記憶部2 0 6に記憶されている許可端末テーブルを参照することにより、問合せメッセージによって特定されている、端末1 0 4の識別子

に対応付けられている接続許可端末の識別子を特定し（ステップS1202）、特定した識別子と問合せ端末103の識別子が一致するか否かにより、端末103が、端末104への接続が許可されている端末に該当するか否かを判定する（ステップS1203）。

- 5 端末103が、端末104への接続が許可されている端末に該当する場合（ステップS1203：Y）、取得要求データを、送信部202を介してアドレス解決サーバ102に送信し（ステップS1204）、アドレス解決サーバ102に図8に示すステップS801～ステップS807の処理を行わせ、アドレス解決サーバ102から端末104のIPアドレスを取得できたか否かを判定する（ステップS1205）。

取得できた場合（ステップS1205：Y）、制御部201は、「接続受入」を示す通知メッセージを、送信部202を介して端末103に送信し（ステップS1206）、端末103に図11に示すステップS1102以降の処理を行わせる。

- 15 さらに、制御部201は、パスワード発行部204にパスワード発行指示を、暗号鍵発行部205に暗号鍵発行指示をし、指示に応じてパスワード発行部204及び暗号鍵発行部205からそれぞれ発行されたパスワード及び暗号鍵と、問合せ端末103の識別子とから、認証情報通知メッセージを作成し（ステップS1207）、作成した認証情報通知メ  
20 ッセージを、送信部202を介して端末104に送信する（ステップS1208）。

- 次に、制御部201は、発行されたパスワードと暗号鍵、及び取得した端末104のIPアドレスとから、接続先通知メッセージを作成し（ステップS1209）、送信部202を介して端末103に送信する（ス  
25 テップS1210）。

又、ステップS1203において、端末103が、端末104への接続が許可されている端末に該当しない場合（ステップS1203：N）、及びステップS1205において、アドレス解決サーバ102から未登録メッセージを受信し、端末104のIPアドレスを取得できなかった

た場合（ステップS 1 2 0 5：N）、「接続拒否」を示す通知メッセージを端末1 0 3に送信する（ステップS 1 2 1 1）。

次に、仲介サーバ1 0 1による端末間の通信データの転送処理の動作について説明する。図2 2は、上記動作を示すフローチャートである。

5 以下、図2 2を参照して、上記動作について説明する。

制御部2 0 1は、受信部2 0 3より通信データ転送通知メッセージを受取ると（ステップS 2 2 0 1）、当該通信データ転送通知メッセージに含まれる通信データのデータサイズ情報に基づいて、通信データのデータサイズが許容通信データサイズ閾値を超えているか否かを判定する（

10 ステップS 2 2 0 2）。

超えていない場合に（ステップS 2 2 0 2：N）、「通信データの受入を許可する」旨の転送受入通知メッセージを作成して、送信部2 0 2を介して当該転送受入通知メッセージを問合せ端末に送信し（ステップS 2 2 0 3）、当該転送受入通知メッセージに応じて当該端末より送信された

15 暗号化通信データを受信部2 0 3を介して受取ると（S 2 2 0 4）、受取った暗号化通信データを送信部2 0 2を介して接続先端末に送信する（ステップS 2 2 0 5）。

ステップS 2 2 0 2において、通信データのデータサイズが許容通信データサイズ閾値を超えている場合（ステップS 2 2 0 2：Y）、制御部

20 2 0 1は、通信データの受入を許可しない」旨の転送受入通知メッセージを作成して、送信部2 0 2を介して当該転送受入通知メッセージを問合せ端末に送信する（ステップS 2 2 0 6）。

次に、図1 1のステップS 1 1 0 7において、端末1 0 3によって接続受入要求された端末1 0 4が行う他端末からの接続受入処理の動作について説明する。図1 3は、上記動作を示すフローチャートである。以下、図1 3を用いて上記動作について説明する。

25

端末1 0 4は、端末1 0 3から接続受入要求される前に、図1 2のステップS 1 2 0 8において、仲介サーバ1 0 1から送信された認証情報通知メッセージを受信すると（ステップS 1 3 0 1）、当該認証情報通知

メッセージから端末103の識別子、パスワード及び暗号鍵を取得する  
(ステップS1302)。

さらに、端末103から、接続受入要求メッセージを受信することにより、接続受入要求を受けると(ステップS1303)、当該接続受入要求  
5 求メッセージを、取得した暗号鍵を用いて復号し、当該接続受入要求メッセージから、端末103の識別子とパスワードを取得し(ステップS1304)、取得した識別子、パスワードについてそれぞれ、先に認証情報通知メッセージから取得した識別子、パスワードとの照合を行い(ステップS1305)、識別子とパスワードの何れもが一致するか否かを判定  
10 する(ステップS1306)。

識別子とパスワードの何れもが一致する場合(ステップS1306: Y)、「接続受入」を示す通知メッセージを作成し(ステップS1307)、取得した暗号鍵を用いて暗号化して、接続受入要求をした端末103に送信し(ステップS1308)、端末103とのデータ通信を開始する  
15 (ステップS1309)。

ステップS1306において、識別子とパスワードの何れかが一致しない場合(ステップS1306: N)、「接続拒否」を示す通知メッセージを作成し(ステップS1310)、取得した暗号鍵を用いて暗号化して、接続受入要求をした端末103に送信し(ステップS1311)、端末  
20 103との接続を中止する(ステップS1312)。

次に、各端末の行なう通信データ送信制御処理の動作について説明する。図23は、上記動作を示すフローチャートである。以下、図23を参照して、上記動作について説明する。

なお、ここでは、説明を簡略化するため、端末103を通信データを  
25 送信する送信元端末とし、端末104を通信データを送信する送信先端末として上記動作について説明する。

端末103は、図13のステップS1309において、端末104との通信を開始後、入力部407を介して、ユーザーから接続先端末に送信すべき通信データの指定を受取ると(ステップS2301)、端末10



3の制御部401は、当該通信データを記憶部406から読出し、記憶部406に記憶されている通信データ秘匿性判定テーブルを参照して、指定された通信データが秘匿性データであるか否かを判定する（ステップS2302）。

- 5 指定された通信データが秘匿性データである場合（ステップS2302：Y）、制御部401は、通信データ転送通知メッセージを作成して、仲介サーバ101及び端末104に送信し（ステップS2303）、仲介サーバ101及び端末104から「通信データの受入を許可する」旨の接続受入通知メッセージを受け取ると（ステップS2304：Y）、読出した通信データを先に受信した接続先通知メッセージに含まれる暗号鍵を用いて暗号化し、仲介サーバ101に送信する（ステップS2305）。

ステップS2302において、指定された通信データが秘匿性データでない場合（S2302：N）、制御部401は、読出した通信データを端末104に直接送信する（ステップS2306）。

- 15 ステップS2304において、仲介サーバ101又は端末104から「通信データの受入を許可しない」旨の接続受入通知メッセージを受け取ると（ステップS2304：N）、制御部401は、通信データ送信制御処理を終了する。

## 20 （実施の形態2）

- 本実施の形態は、第1の実施の形態における動作と比較して、仲介サーバ（実施の形態2においては、仲介サーバ111）が接続先端末と通信する前に、当該端末の状態を問い合わせ、当該端末が通信を受入可能な状態にあるか否かを判定し、受け入れ不可能な状態にある場合はそれを問合せ端末に通知する点が異なる。実施の形態1における通信システム100と同一の構成要素については、同一の番号を付し、以下、第1の実施の形態との相違点を中心に説明する。

図14は、本発明の実施の形態2における通信システム110の構成を示す機能ブロック図である。通信システム110は、仲介サーバ11

1、アドレス解決サーバ102、端末103、端末114とから構成され、各構成要素はインターネット105で接続されている。

図15は、仲介サーバ111の構成を示す機能ブロック図である。

仲介サーバ111は、制御部211、送信部202、受信部203、  
5 パスワード発行部204、暗号鍵発行部205、記憶部206から構成される。

制御部211の行う動作は、第1の実施の形態における制御部201の動作と比較して、接続制御処理の動作において異なる。以下、制御部211の行う接続制御処理の動作について、図12に示す接続制御処理  
10 の動作との相違点を中心に説明する。図16は、上記動作を示すフローチャートである。以下、図16を参照して、上記動作について説明する。

ステップS1201～ステップS1205までの処理については、図12の実施の形態1における動作と同じであるので、説明を省略する。

15 ここで、図16のステップS1201～ステップS1210の各ステップにおける処理は、端末104を端末114に読み替えると、図12における各同一番号のステップにおける処理と同一であるので、各ステップ間の対応関係を明確にするため、図12における対応するステップ番号と同一のステップ番号を付している。

20 制御部211は、ステップS1201～ステップS1205までの処理を行った後、ステップS1205において、端末114のIPアドレスを取得できた場合（ステップS1205：Y）、端末114に、当該端末が接続受入状態にあるか否かを問い合わせるための受入状態問合せメッセージを送信し（ステップS1606）、当該端末から返答を示す通知  
25 メッセージを受信すると（ステップS1607）、当該通知メッセージを解析して、当該通知メッセージが「接続受入状態にある」ことを示しているか否かを判定する（ステップS1608）。

図17（a）は、上記において、端末114に送信される受入状態問合せメッセージの具体例を示す。ここでは、「QUERY」は、問合せメッセ

ージであることを示し、「STATUS」は、問合せの内容が、接続受入状態であることを示している。

図17(b)、及び図17(c)は、端末114から受信する返答を示す通知メッセージの具体例を示す。ここでは、「NOTIFY」は、通知メッセージであることを示し、図17(b)の「STATUS Acceptable」は、「接続受入状態にある」ことを示し、図17(c)の「STATUS Busy」は、「接続拒否状態にある」ことを示している。

当該通知メッセージが「接続受入状態にある」ことを示している場合(ステップS1608:Y)、制御部211は、図12のステップS1206～ステップS1210と同じ処理を行い、当該通知メッセージが「接続受入拒否の状態にある」ことを示している場合(ステップS1608:N)、図12のステップS1211と同じ処理を行う。

端末114は、端末104の有する機能に加え、一定時間内のCPUのRAMへのアクセス回数を継続的に測定することにより、CPUの負荷量を測定し、さらに、負荷量の上限を示すCPU負荷上限値を記憶している。

具体的には、端末114は、制御部411、送信部402、受信部403、暗号化部404、復号化部405、記憶部416、入力部407から構成され、制御部411は、制御部401の有する機能に加え、CPUの負荷量を測定する機能を有し、記憶部416は、記憶部406の有する機能に加え、CPU負荷上限値を記憶している。図30は、端末114の構成を示す機能ブロック図である。

次に、上記の制御部211による接続制御処理に伴って、端末114が、図13に示す接続受入処理と同一の処理を行う前に実行する接続受入状態の通知処理の動作について説明する。図18は、上記動作を示すフローチャートである。以下、図18を参照して、上記動作について説明する。

端末114は、図16のステップS1606において、仲介サーバ111から送信された受入状態問合せメッセージを受信すると(ステップ

S 1 8 0 1)、CPUの負荷量がCPU負荷上限値を超えているか否かを判定する(ステップS 1 8 0 2)。

- 5 超えていない場合(ステップS 1 8 0 2 : N)、「接続受入状態にある」ことを示す通知メッセージを、仲介サーバ1 1 1に送信し(ステップS 1 8 0 3)、超えている場合(ステップS 1 8 0 2 : Y)、「接続拒否状態にある」ことを示す通知メッセージを、仲介サーバ1 1 1に送信する(ステップS 1 8 0 4)。

### (実施の形態3)

- 10 本実施の形態は、第2の実施の形態における動作と比較して、接続先端末が問合せ端末と通信不可能な状態にある場合に、問合せ端末からの通信データ保管依頼に応じて仲介サーバ(実施の形態3においては、仲介サーバ1 2 1)が当該通信データを一時的に保管し、接続先端末が通信可能な状態になった時に、保管していた通信データを接続先サーバに
- 15 転送する処理を行なうという点が異なる。実施の形態2における通信システム1 1 0と同一の構成要素については、同一の番号を付し、以下、第2の実施の形態との相違点を中心に説明する。

- 図2 4は、本発明の実施の形態3における通信システム1 2 0の構成を示す機能ブロック図である。通信システム1 2 0は、仲介サーバ1 2
- 20 1、アドレス解決サーバ1 0 2、端末1 2 3、端末1 2 4とから構成され、各構成要素はインターネット1 0 5で接続されている。

図2 5は、仲介サーバ1 2 1の構成を示す機能ブロック図である。

- 仲介サーバ1 2 1は、制御部2 2 1、送信部2 0 2、受信部2 0 3、パスワード発行部2 0 4、暗号鍵発行部2 0 5、記憶部2 2 6から構成
- 25 される。

制御部2 2 1の行う動作は、第2の実施の形態における制御部2 1 1の動作と比較して、接続制御処理の動作において異なる。以下、制御部2 2 1の行う接続制御処理の動作について、図1 6に示す接続制御処理の動作との相違点を中心に説明する。図2 6及び図2 7は、上記動作を

示すフローチャートである。以下、図 26 を参照して、上記動作について説明する。

ここで、図 26 のステップ S 1 2 0 1 ～ステップ S 1 2 1 0 の各ステップにおける処理及びステップ S 1 6 0 6 ～ステップ S 1 6 0 8 の処理は、端末 1 1 4 を端末 1 2 4 に読み替えると、図 16 における各同一番号のステップにおける処理と同一であるので、各ステップ間の対応関係を明確にするため、図 16 における対応するステップ番号と同一のステップ番号を付している。

制御部 2 2 1 は、ステップ S 1 2 0 1 ～ S 1 2 0 5、S 1 6 0 6 ～ S 1 6 0 8 までの処理を行なった後、ステップ S 1 6 0 8 において、端末 1 2 4 から受信した返答を示す通知メッセージが「接続受入状態にない」ことを示している場合（ステップ S 1 6 0 8 : N）、通信データの転送を依頼するか否かについて端末（ここでは、端末 1 2 3）に問合せするための転送依頼問合せメッセージを作成して送信部 2 0 2 を介して端末 1 2 3 に送信し（ステップ S 2 6 1 1）、端末 1 2 3 から当該転送依頼問合せメッセージに対する返答通知メッセージである転送依頼問合せ返答通知メッセージを受信部 2 0 3 を介して取得し（ステップ S 2 6 1 2）、当該転送依頼問合せ返答メッセージを解析して、当該転送依頼問合せ返答通知メッセージが「通信データの転送依頼をする」ことを示しているか否かを判定する（ステップ S 2 6 1 3）。

ここで、「転送依頼問合せメッセージ」とは、制御部 2 2 1 によって作成される、端末（ここでは、端末 1 2 3）に、通信データの転送を依頼するか否かについて問合せるメッセージのことをいい、問合せメッセージであることを示す識別子と問合せ元である仲介サーバ 1 2 1 の識別子と問合せ内容と端末 1 2 3 の IP アドレスとを含むメッセージのことをいう。

又、「転送依頼問合せ返答通知メッセージ」とは、端末（ここでは端末 1 2 3）によって作成される、転送依頼問合せメッセージに対する返答メッセージのことをいい、通知メッセージであることを示す識別子と送

信元端末である端末１２３の識別子と仲介サーバ１２１のＩＰアドレスと返答内容とを含むメッセージのことをいう。

- 当該転送依頼問合せ返答メッセージが「通信データの転送依頼をする」ことを示している場合（ステップＳ２６１３：Ｙ）、通信データ送信要求メッセージを作成して送信部２０２を介して端末１２３に送信し（ステップＳ２６１４）、さらに、転送依頼通知メッセージを作成して送信部２０２を介して端末１２４に送信し（ステップＳ２６１５）、端末１２３から通信データを受信部２０３を介して取得すると（ステップＳ２６１６）、当該通信データを送信元である端末１２３の識別子と送信先である
- 5 端末１２４の識別子と対応付けて記憶部２２６に記録し（ステップＳ２  
10 ６１７）、端末１２４から転送依頼データ転送要求メッセージを受信部２  
０３を介して取得すると（ステップＳ２６１８）、記憶部２２６から、当  
該転送依頼データ転送要求メッセージに含まれる送信元の端末の識別子  
及び送信先の端末の識別子に対応付けられている通信データを読み出し、
- 15 送信部２０３を介して端末１２４に転送する（ステップＳ２６１９）。

ここで、「通信データ送信要求メッセージ」とは、制御部２２１によって作成され、通信データの転送を依頼する端末（ここでは、端末１２３）に送信される、転送を依頼する通信データの送信を要求するメッセージのことをいい、要求メッセージであることを示す識別子と要求内容と

20 要求元である仲介サーバ１２１の識別子と端末１２３のＩＰアドレスとを含むメッセージのことをいう。

又、「転送依頼通知メッセージ」とは、制御部２２１によって作成され、問い合わせ端末（ここでは、端末１２３）から通信データの転送依頼があったことを通知するメッセージのことをいい、通知メッセージであることを示す識別子と通知内容と通知元である仲介サーバ１２１の識別子と転送依頼元の端末（ここでは、端末１２３）の識別子と端末１２４のＩＰアドレスとを含むメッセージのことをいう。

25

又、「転送依頼データ転送要求メッセージ」とは、転送要求元端末（ここでは、端末１２４）によって作成されて送信される、仲介サーバ１２

1に保管している通信データの転送を要求するメッセージのことをいい、要求メッセージであることを示す識別子と要求内容と通信データの転送依頼元の端末の識別子（ここでは、端末123）と転送要求元の端末（ここでは、端末124）の識別子と仲介サーバ121のIPアドレス  
5 とを含むメッセージのことをいう。

次に、仲介サーバ121によるステップS2611による処理を介して送信された転送依頼問合せメッセージを端末123が受信した場合に、端末123が行なう通信データ転送依頼処理の動作について説明する。  
10 端末123は、図31に示すように制御部421、送信部402、受信部403、暗号化部404、復号化部405、記憶部406、入力部407から構成され、制御部421は、制御部411の有する機能に加え、上記動作を行なう。

なお、制御部421は、後述する端末124の制御部431の機能を備えることとしてもよい。

15 又、記憶部406は、後述する記憶部436の機能を備えることとしてもよい。

図28は、上記動作を示すフローチャートである。

以下、図28を参照して、上記動作について説明する。

制御部421は、仲介サーバ121から送信された転送依頼問合せメッセージを受信部403を介して取得すると（ステップS2801）、入力部407から入力されるユーザー指示に基づいて転送依頼問合せ返答通知メッセージを作成し（ステップS2802）、仲介サーバ121に送信し（ステップS2803）、仲介サーバ121から通信データ転送要求  
20 メッセージを受信すると（ステップS2804）、入力部407から入力されるユーザー指示に基づいて、記憶部406に記憶されている各種通信データの中から指示された通信データを読み出し、仲介サーバ121に送信する（ステップS2805）。  
25

次に、仲介サーバ121によるステップS2615による処理を介して送信された転送依頼通知メッセージを端末124が受信した場合に、

端末 1 2 4 が行なう通信データ受入制御処理の動作について説明する。

端末 1 2 4 は、図 3 2 に示すように制御部 4 3 1、送信部 4 0 2、受信部 4 0 3、暗号化部 4 0 4、復号化部 4 0 5、記憶部 4 3 6、入力部 4 0 7 から構成され、制御部 4 3 1 は、制御部 4 1 1 の有する機能に加え

5 、上記動作を行なう。

なお、制御部 4 3 1 は、制御部 4 2 1 の有する機能を備えることとしてもよい。

又、記憶部 4 3 6 は、記憶部 4 1 6 の有する機能に加え、転送依頼元リストを記憶している。

10 ここで、「転送依頼元リスト」とは、仲介サーバ 1 2 1 から、転送依頼通知メッセージを介して通知された通信データの転送依頼元の端末の識別子のリストのことをいい、転送依頼通知メッセージが端末 1 2 4 に通知される毎に、当該転送依頼通知メッセージに含まれる転送依頼元の端末の識別子が制御部 4 3 1 によって抽出され、リストに追加され、リ  
15 ストに含まれる転送依頼元からの通信データが制御部 4 3 1 によって取得される毎に、当該転送依頼元の識別子がリストから制御部 4 3 1 によって削除される。

図 2 9 は、上記動作を示すフローチャートである。

制御部 4 3 1 は、受信部 4 0 3 を介して転送依頼通知メッセージを取  
20 得すると（ステップ S 2 9 0 1）、当該転送依頼通知メッセージから転送依頼元の識別子を取得して、記憶部 4 3 6 の転送先依頼元リストに追加し（ステップ S 2 9 0 2）、CPU の負荷量が CPU 負荷上限値を超えているか否かにより、転送依頼されている通信データを取得可能な状態になったか否かを判定する（ステップ S 2 9 0 3）。

25 超えていない場合、通信データを取得可能な状態になったと判定し（ステップ S 2 9 0 3：Y）、制御部 4 3 1 は、記憶部 4 3 6 に記憶されている転送依頼元リストを参照して、当該転送依頼元リストに転送依頼元の識別子が記録されているか否かにより、転送待ちの通信データが仲介サーバ 1 2 1 に保管されているか否かを判定する（ステップ S 2 9 0 4



。)

転送依頼元の識別子が記録されている場合、転送待ちの通信データが仲介サーバ121に保管されていると判定し（ステップS2904：Y）、当該転送依頼元の識別子に基づいて転送依頼データ転送要求メッセージを作成して送信部402を介して仲介サーバ121に送信し（ステップS2905）、当該転送依頼元の端末から転送依頼された通信データを仲介サーバ121から受信部403を介して取得し、取得した通信データを記憶部436に記録する（ステップS2906）。

ステップS2903において、CPUの負荷量がCPU負荷上限値を超えている場合、通信データを取得可能な状態になっていないと判定し（ステップS2903：N）、制御部431は、CPU負荷量の測定を継続し（ステップS2907）、ステップS2903の処理に移行する。

以上、本発明の実施の形態について説明したが、本発明はこの実施の形態に限定されないのは言うまでもない。

（1）実施の形態1～3においては、仲介サーバとアドレス解決サーバは、別々の独立した、通信システム100、110、及び120の構成要素としたが、仲介サーバがアドレス解決サーバの機能を備えることとし、通信システム100、110、及び120において、アドレス解決サーバーを含まない構成としてもよい。

具体的には、仲介サーバ101又は111又は121が、インターネットに接続している各端末から送信された、当該端末のIPアドレス及び識別子を受信部203を介して取得し、IPアドレス対応テーブルを作成し、記憶部206に登録することとしてもよい。

（2）実施の形態1～3においては、各端末のIPアドレスのIPアドレス対応テーブルへの登録は、アドレス解決サーバ102が、各端末からアドレス解決サーバに直接送信された、当該端末のIPアドレス及び識別子に基づいて行われることとしたが、仲介サーバ101又は111又は121が、各端末から送信された、当該端末のIPアドレス及び識別子を受信し、アドレス解決サーバ102に送信することにより、上記

登録がアドレス解決サーバ 102 において、行われることとしてもよい。

又、アドレス解決サーバ 102 が、各端末から直接、又は仲介サーバ 101 又は 111 又は 121 を介して当該端末の識別子のみを受信し、  
5 当該識別子の端末の IP アドレスを、当該識別子の端末に IP アドレスを割当てたプロバイダーのサーバに問合せ、当該サーバから IP アドレスを取得し、IP アドレス対応テーブルに登録することとしてもよい。

(3) 実施の形態 1～3 においては、アドレス解決サーバ 102 は、端末の識別子を当該端末の IP アドレスと対応付けて IP アドレス対応テーブルに登録することとしたが、各端末から IP アドレスではなく、IP アドレスを特定する情報（例えば、ドメイン名）を取得し、IP アドレス対応テーブルに登録することとし、仲介サーバ 101 又は 111 に対し、当該特定情報を、当該仲介サーバからの取得要求データに対する  
10 返答として、送信することとしてもよい。この場合、当該特定情報を取得した仲介サーバは、例えば、DNS サーバに当該特定情報に対応する IP アドレスを問合せることにより、IP アドレスを取得することとしてもよい。

(4) 実施の形態 1～3 において、各端末を識別する識別子としては、  
20 各端末を区別できるものであればよく、例えば、電話番号、利用者の氏名と住所の組み合わせなど、利用者にとって覚えやすいものを用いることとしてもよい。

又、特定の端末グループを表す識別子を用いて、接続許可を登録することとしてもよい。これにより、各端末は、当該識別子を接続許可端末の識別子として、仲介サーバ 101 又は 110 に登録することにより、  
25 特定のグループ単位で接続許可を付与することができる。

(5) 実施の形態 1～3 において、図 11 のステップ S1101 及び図 12 又は図 16 又は図 26 のステップ S1201 の示す問合せメッセージの送受信を行う前に、端末 103 の認証処理を行うこととしてもよい。

。具体的には、端末 103 は、問合せメッセージを送信する前に当該端末の識別子と認証用のパスワードを送信し、仲介サーバ 101 又は 111 又は 121 は、受信したパスワードと、予め記憶部 206 又は 226  
5 に、端末 103 又は 123 の識別子と対応付けて記憶している照合用パスワードとの照合を行うことにより、端末 103 の認証処理を行い、パスワードが一致する場合に、図 12（仲介サーバ 111 の場合は図 16、仲介サーバ 121 の場合は図 26）のステップ S1201 以降の処理を行うこととしてもよい。

10 又、上記と同様の認証処理を、端末 104 又は 114 又は 124 と仲介サーバ 101 又は 111 又は 121 が通信を開始する際に行うこととしてもよい。

又、認証の方法は上記以外の方法であってもよい。例えば、認証局が発行した証明書を取り交わすことであってもよい。

15 （6）実施の形態 1 及び 2 における図 12 及び図 16 に示す仲介サーバの接続制御処理の動作において、ステップ S1203、ステップ S1205（以上、図 12 及び図 16）、及びステップ S1608（図 16）の判定において、判定結果が「否定」である場合に、何れの場合においても図 5（c）に示す、「接続拒否」の通知メッセージを端末 103 に送信  
20 する（ステップ S1211）こととしたが、各ステップ毎に送信する通知メッセージの内容を異なるものとしてもよい。

例えば、ステップ S1203 において、図 5（c）、ステップ S1205 において、図 5（g）、ステップ 1608 において、図 5（h）にそれぞれ示す通知メッセージを端末 103 に送信することとしてもよい。

25 或いは、各ステップにおいて、接続拒否の原因を通知するメッセージを送信することとしてもよい。

例えば、ステップ S1203 において、「接続先端末に許可されている端末に該当しない」旨の通知メッセージを送信し、ステップ S1205 において、「接続先端末の IP アドレスが取得できなかった」旨の通知メ

ッセージを送信し、ステップS1608において、「接続先端末が接続受入状態にない」旨の通知メッセージを送信することとしてもよい。

これにより、問合せ端末側において、接続先端末に接続できない原因を知ることができる。

- 5     (7) 実施の形態1～3において、各端末と仲介サーバ101又は111又は121との通信は、SSL (Secure Socket Layer) 又はTSL (Transport Layer Security) プロトコルを用いて行うこととしてもよい。

これにより、データの盗聴を有効に防止することができる。

- 10    (8) 実施の形態1～3において、端末104又は端末114が端末103からの接続を受付けるポート番号又は端末124が端末123からの接続を受付けるポート番号は、予め決められたポート番号（例えば、国際的に取り決められているWell-known Port Number）を用いることとしてもよいし、アドレス解決サーバ102の記憶部304に記憶されているIPアドレス対応テーブルにIPアドレスとともに登録し、仲介サーバ101又は111又は121を介して端末103又は123が接続先端末（端末104又は端末114又は124）の接続受け付けポート番号を受取ることもよい。

- 15    このように、接続先端末毎に固有の接続受け付けポート番号を登録することができるので、固有のポート番号を指定する端末からのアクセスのみを受け入れることができ、他の端末からの不正アクセスを有効に防止することができる。

- 25    (9) 実施の形態1～3において、図13のステップ1305におけるパスワードの照合は、接続受入要求先の端末の側だけでなく、接続受入要求元の端末の側においても、接続要求先の端末から当該パスワードを取得することにより、行うこととしてもよい。

この場合、両者の端末において、パスワードが一致する場合に、ステップS1307～ステップS1309の処理を行うこととしてもよい。

なお、上記の場合、両者の端末において、それぞれ照合に用いるパス

ワードは、異なるものである。

(10) 実施の形態1における通信データ送信制御処理において、制御部401は、ユーザーによって指定された通信データが秘匿性データであるか否かにより、当該通信データを仲介サーバ101を介して接続先  
5 端末に送信するか否かの決定をすることとしたが、指定された通信データのデータサイズによって上記決定をすることとしてもよい。

又、実施の形態2及び3においても、制御部411、421、431が通信データ制御処理において、指定された通信データのデータサイズによって上記決定をすることとしてもよい。

10 例えば、通信データが動画を構成する、データサイズの大きいデータの場合には、直接接続先端末に通信データを送信することとし、テキストデータや静止画を構成するデータのようにデータサイズの小さいデータの場合には、仲介サーバ101を介して通信データを接続先サーバに送信することとしてもよい。

15 具体的には、各通信データと当該通信データのデータサイズとの対応関係を示す通信データサイズ判定テーブルを予め記憶部406に記録しておき、制御部401は、入力部407を介してユーザーから接続先端末に送信すべき通信データの指定を受取ると、通信データサイズ判定テーブルを参照して、当該通信データのデータサイズが所定の閾値を超えるか否かを判定し、超えない場合に、当該通信データを仲介サーバ10  
20 1を介して送信することを決定し、超える場合に、当該通信データを直接接続先サーバに送信することを決定することとしてもよい。

又、制御部401は、指定された通信データの一部を仲介サーバ101を介して送信し、指定された通信データの残りの部分を直接接続先サーバに送信することを決定することとしてもよい。実施の形態2及び3  
25 においても、端末の制御部411、421、431がそれぞれ、上記と同様の決定をすることとしてもよい。

例えば、MPEG (Moving Picture Expert Group) - 2の規格に従ったフレーム間の予測を用いて圧縮された、1つのIピクチャと複数のB

- ピクチャ、Pピクチャから成るGOP (Group of Picture) 単位で構成される映像データストリームが通信データとして記憶部406に記録されている場合に、当該映像データストリームが接続先端末に送信すべき通信データとしてユーザーによって指定されると、制御部401は、映像データストリームを構成する各ピクチャに、当該ピクチャの映像データストリームにおける順序に対応する連続番号を付与し、映像データストリームからIピクチャを抽出して、接続先通知メッセージに含まれる暗号鍵を用いて暗号化し、仲介サーバ101に暗号化した各Iピクチャの転送依頼をして、暗号化した各Iピクチャを仲介サーバ101に送信し、さらに仲介サーバ101を介して抽出した各Iピクチャを接続先端末に送信し、残りの各Bピクチャ及び各Pピクチャを直接接続先端末に送信することを決定することとしてもよい。実施の形態2及び3においても、端末の制御部411、421、431がそれぞれ、上記と同様の決定をすることとしてもよい。
- 15     なお、通信データが映像ストリームであるか否かの判定は、例えば、各通信データと当該通信データのデータの種類の対応関係を示す通信データ種判定テーブルを予め記憶部406に記録しておき、制御部401が、入力部407を介してユーザーから接続先端末に送信すべき通信データの指定を受取ったときに、通信データ種判定テーブルを参照することにより行うこととしてもよい。
- 20

これにより、Iピクチャ以外の通信データは、暗号化されることなく、直接送信されるので、接続先端末における通信データの暗号の復元が不要となるので、その分だけ通信データの復号に要する負荷が少なくでき、又、映像データの再生に必要不可欠なIピクチャは、暗号化された後、送信されるので、何らの原因で通信データが他人によって搾取された場合においても、Iピクチャが暗号化されているため、搾取された通信データが他人によって勝手に再生されることを防止することができる。

(11) 実施の形態2において、仲介サーバ111は、受入状態問合せ

メッセージを端末 1 1 4 に送信する際に、端末 1 1 4 との接続が確立できない場合においても、「接続拒否」を示す通知メッセージを端末 1 0 3 に送信することとしてもよい。

具体的には、図 1 6 のフローチャートのステップ S 1 2 0 5 とステップ S 1 6 0 6 との間に、図 1 9 に示す接続確立判定処理の動作（ステップ S 1 9 0 1 及びステップ S 1 9 0 2）を加えることとしてもよい。

以下、図 1 9 を参照して、上記動作について説明する。

図 1 6 のステップ S 1 2 0 5 において、接続先端末 1 1 4 の IP アドレスが取得できた場合（ステップ S 1 2 0 5 : Y）、制御部 2 1 1 は、端末 1 1 4 との接続を試み（ステップ S 1 9 0 1）、接続できた場合（ステップ S 1 9 0 2 : Y）、図 1 6 に示すステップ S 1 6 0 6 以降の処理を行い、接続できなかった場合（ステップ S 1 9 0 2 : N）、図 1 6 のステップ S 1 2 1 1 の処理を行う。

（1 2）実施の形態 2 において、端末 1 1 4 は、CPU 負荷量を測定し、測定した CPU 負荷量が CPU 負荷上限値を超えるか否かにより、接続受入可否の判定を行うこととしたが（図 1 8 のステップ S 1 8 0 2）、CPU 負荷量を測定する方法以外の方法によって接続受入可否の判定を行うこととしてもよい。例えば、端末 1 1 4 が、受入状態問合せメッセージ受信時において、他の端末と通信中であるか否かを判定し、通信中でない場合に「接続受入状態にある」ことを示す通知メッセージを仲介サーバ 1 1 1 に送信し、通信中である場合に、「接続拒否状態にある」ことを示す通知メッセージを仲介サーバ 1 1 1 に送信することとしてもよい。

又、実施の形態 3 においても、端末 1 2 4 が、端末 1 1 4 の場合と同様に受入状態問合せメッセージ受信時において、他の端末と通信中であるか否かを判定し、当該判定結果に基づいて上記と同様にして通知メッセージを仲介サーバ 1 2 1 に送信することとしてもよい。

（1 3）実施の形態 1 ～ 3 において、通信データの送受信を行なう通信プロトコルとしては、例えば、HTTP (Hyper Text Transfer Protocol)

1)、R T P (Real-Time Transport Protocol)、R T S P (Real-Time Streaming Protocol)／R T P (Real-Time Transport Protocol)、F T P (File Transfer Protocol)などの通信プロトコールを使用することができる。

- 5 又、実施の形態 1 ～ 3 において、映像データ、音声データ、画像データなどのマルチメディアデータを通信する場合には、データ通信の制御プロトコールとしてU P n P A Vによって規定されるプロトコールを使用することができる。

- 10 ここで、U P n P (Universal Plug&Play)とは、U P n P F o r u m で策定された、パソコンや周辺機器などネットワークに接続された機器が、お互いに認識しあい機能するための技術仕様であり、U P n P A V (UPnP AV Architecture)とは、U P n P の上で、デジタルコンテンツをホームネットワーク内で転送、再生する方法として策定された規格である。

- 15 (14) 実施の形態 1 ～ 3 の各通信システムにおいては、端末間の接続が確立された後に、送信元の端末からの依頼に応じて、仲介サーバが依頼された通信データを送信先の端末へ転送する通信データの転送処理を行なうこととしたが、各通信システムは、上記転送処理を行なわないものであってもよい。



## 請 求 の 範 囲

1. 第1及び第2通信端末と、第2通信端末のネットワーク上における  
アドレスを特定するための宛先情報を通知する通信制御サーバとから構  
5 成される通信システムであって、  
第1通信端末は、前記宛先情報を要求する要求メッセージを前記通信  
制御サー  
バに送信し、  
前記通信制御サーバは、  
10 第2通信端末と、第2通信端末への接続が許可された接続許可通信端  
末との対応関係を示す許可端末テーブルを記憶している許可端末テー  
ブル記憶手段と、  
前記要求メッセージを受信する要求メッセージ受信手段と、  
受信した前記要求メッセージを送信した第1通信端末が、第2通信端  
15 末に対応  
付けられている接続許可通信端末に該当するか否かを、前記許可端末テ  
ーブルに基づいて判定する端末判定手段と、  
第1通信端末が第2通信端末に対応付けられている接続許可通信端末  
に該当する場合に限り、第2通信端末の宛先情報を、第1通信端末に通  
20 知する通知制御手段と  
を有することを特徴とする通信システム。
2. 前記通知制御手段はさらに、第1通信端末が第2通信端末への接続  
が許可されている通信端末である場合に限り、第2通信端末が第1通信  
25 端末を認証するための認証情報を作成する認証情報作成手段を有し、  
前記通知制御手段はさらに、前記認証情報を、第1通信端末と第2通  
信端末に通知し、  
第1通信端末は、第2通信端末への接続要求時に、通知された認証情  
報を第2通信端末に送信し、

第2通信端末は、

第1通信端末から前記認証情報を受信する受信手段と、

受信した認証情報と通知された認証情報とが一致するか否かを判定する判定手段と、

- 5 両者の認証情報が一致する場合に限り、第1通信端末からの接続を許可する接続制御手段と

を有することを特徴とする請求の範囲第1項記載の通信システム。

3. 前記通知制御手段はさらに、第1通信端末と第2通信端末間で送受信される情報を暗号化及び復号化するための暗号鍵を作成する暗号鍵作成手段を有し、

前記通知制御手段はさらに、前記暗号鍵を第1通信端末と第2通信端末に通知する

ことを特徴とする請求の範囲第1項に記載の通信システム。

15

4. 前記通知制御手段はさらに、第2通信端末の宛先情報を第1通信端末に通知する前に、第2通信端末が第1通信端末からの接続を受入可能か否かについての問合せメッセージを第2通信端末に送信し、

第2通信端末は、

- 20 前記問合せメッセージを受信する受信手段と、

前記問合せメッセージの受信時における負荷状態に応じて、第1通信端末からの接続の受入可否を判定し、判定結果を示す受入可否通知メッセージを前記通信制御サーバに通知する接続受入可否通知手段と

を有し、

- 25 前記通知制御手段は、通知された受入可否通知メッセージに基づいて、第2通信端末が、第1通信端末からの接続を受入可能な状態にあるか否かを判定する接続受入可否判定手段を有し、

第2通信端末が、第1通信端末からの接続を受入可能な状態にある場合に限り、前記通知制御手段は、第2通信端末の宛先情報を第1通信端

末に通知する

ことを特徴とする請求の範囲第 1 項に記載の通信システム。

5. 前記通知制御手段は、第 1 通信端末が第 2 通信端末に接続を許可されている通信端末でない場合に、その旨を示す第 1 通知メッセージを第 1 通信端末に通知し、

第 2 通信端末が、第 1 通信端末からの接続を受入可能な状態にない場合に、その旨を示す第 2 通知メッセージを第 1 通信端末に通知する

ことを特徴とする請求の範囲第 4 項記載の通信システム。

10

6. 通信制御サーバとネットワークで接続された通信端末であって、

前記通信制御サーバに、前記通信端末への接続が許可された通信端末の登録要求をする許可通信端末登録要求手段と、

- 15 前記通信端末のネットワーク上におけるアドレスを特定するための宛先情報を要求した通信端末が前記通信端末への接続が許可された通信端末である場合に限り、前記通信制御サーバから送信される、前記宛先情報を要求した通信端末を認証するための認証情報を受信する認証情報受信手段と、

- 20 前記宛先情報を要求した通信端末から、接続受入要求と当該通信端末を識別するための識別情報を受信する識別情報受信手段と、

前記認証情報と前記識別情報とが一致するか否かを判定する判定手段と、

- 25 前記認証情報と前記識別情報とが一致する場合に限り、前記宛先情報を要求した通信端末からの接続受入要求に基づく接続を許可する接続制御手段と

を備えることを特徴とする通信端末。

7. 前記識別情報受信手段はさらに、前記接続受入要求が送信される前に、前記宛先情報を要求した通信端末からの接続を受入可能か否かにつ

いての問合せメッセージを、前記通信制御サーバから受信し、

前記接続制御手段は、前記問合せメッセージの受信時における負荷状態に応じて、前記接続が受入可能か否かを判定し、判定結果を前記通信制御サーバに通知する

5     ことを特徴とする請求の範囲第6項記載の通信端末。

8. 前記識別情報受信手段は、前記宛先情報を要求した通信端末からの接続を受入可能な状態にない場合に、前記通信制御サーバから、前記宛先情報を要求した通信端末からの通信データの転送依頼があったことを

10    通知する転送依頼通知メッセージを受信し、

前記通信端末は、

負荷状態に応じて前記通信データを取得可能な状態になったか否かを判定する通信データ取得可否判定手段と、

前記転送依頼通知メッセージが受信された後に、前記通信データを取得可能な状態になった場合に、前記通信データの転送を要求する転送要求メッセージを前記通信制御サーバに送信する転送要求メッセージ送信手段と、

15    前記転送要求メッセージに応じて前記通信制御サーバから送信された前記通信データを取得する取得手段と

20    を備えることを特徴とする請求の範囲第7項記載の通信端末。

9. 前記通信端末はさらに、

接続先通信端末に送信すべき各種通信データを当該通信データのデータ属性と対応付けて記憶している記憶手段と、

25    前記接続先通信端末のネットワーク上におけるアドレスを特定するための宛先情報を要求する要求メッセージを前記通信制御サーバに送信する送信手段と、

前記通信端末が前記接続先通信端末によって接続が許可された通信端末である場合に限り、前記通信制御サーバから通知される前記宛先情報

を取得する取得手段と、

取得された前記宛先情報に基いて、前記接続先通信端末との接続を確立する接続確立手段と、

送信すべき通信データの指定を受取る指定受取手段と、

- 5 指定された通信データが特定のデータ属性を有するか否か判定するデータ属性判定手段と、

指定された通信データが特定のデータ属性を有する場合に、前記通信制御サーバに、指定された通信データの前記接続先通信端末への転送を依頼する転送依頼手段と、

- 10 指定された通信データが特定のデータ属性を有する場合に、指定された通信データを前記通信制御サーバに送信し、指定された通信データが特定のデータ属性を有しない場合に、指定された通信データを接続している前記接続先通信端末に直接送信する制御を行なう送信制御手段と  
を備えることを特徴とする請求の範囲第6項記載の通信端末。

15

10. 前記送信制御手段は、

指定された通信データがMPEG符号化された映像データである場合に、当該映像データからIピクチャを抽出する抽出手段と、

抽出したIピクチャを暗号化する暗号化手段と

- 20 を有し、

前記転送依頼手段は、暗号化されたIピクチャの前記接続先通信端末への転送を依頼し、

前記送信制御手段は、暗号化したIピクチャを前記通信制御サーバに送信し、Iピクチャを除く残りの映像データを接続している前記接続先

- 25 通信端末に直接送信する

ことを特徴とする請求の範囲第9項に記載の通信端末。

11. 前記データ属性は、通信データの秘匿性の有無を示すデータ属性であり、

前記転送依頼手段は、指定された通信データのデータ属性が秘匿性の有ることを示している場合に、前記通信制御サーバに、指定された通信データの前記接続先通信端末への転送を依頼し、

5 前記送信制御手段は、指定された通信データのデータ属性が秘匿性の有ることを示している場合に、指定された通信データを暗号化して前記通信制御サーバに送信する

ことを特徴とする請求の範囲第9項記載の通信端末。

12. 前記アドレスは、IPアドレスである

10 ことを特徴とする請求の範囲第6項～第11項の何れかに記載の通信端末。

13. 前記アドレスは、IPアドレスとポート番号とから構成される

15 ことを特徴とする請求の範囲第6項～第11項の何れかに記載の通信端末。

14. 前記アドレスは、随時変動する

ことを特徴とする請求の範囲第6項～第13項の何れかに記載の通信端末。

20

15. 通信端末のアドレスを特定するための宛先情報を通知する通信制御サーバであって、

前記通信端末と、当該通信端末への接続が許可された通信端末との対応関係を示す許可端末テーブルを記憶している許可端末テーブル記憶手

25 段と、

前記宛先情報を要求する要求メッセージを要求元通信端末から受信する要求

メッセージ受信手段と、

前記要求元通信端末が、前記通信端末に接続を許可されている通信端

末である

か否かを、前記許可端末テーブルに基づいて判定する端末判定手段と、

前記要求元通信端末が、接続を許可されている通信端末である場合に限り、前記通信端末の宛先情報を前記要求元通信端末に通知する通知制

5 御手段と

を備えることを特徴とする通信制御サーバ。

16. 通信制御サーバとネットワークで接続された通信端末に用いる接続制御プログラムであって、

10 前記接続制御プログラムは、

前記通信制御サーバに、当該通信端末への接続が許可された通信端末の登録要求をする許可通信端末登録要求ステップと、

前記通信端末のネットワーク上におけるアドレスを特定するための宛先情報を要求した通信端末が前記通信端末への接続が許可された通信  
15 端末である場合に限り、前記通信制御サーバから送信される、前記宛先情報を要求した通信端末を認証するための認証情報を受信する認証情報受信ステップと、

前記宛先情報を要求した通信端末から、接続受入要求と当該通信端末を識別するための識別情報を受信する識別情報受信ステップと、

20 前記認証情報と前記識別情報とが一致するか否かを判定する判定ステップと、

前記認証情報と前記識別情報とが一致する場合に限り、前記宛先情報を要求した通信端末からの接続受入要求に基づく接続を許可する接続制御ステップと

25 を含むことを特徴とする接続制御プログラム。

17. 通信制御サーバとネットワークで接続された通信端末に用いる接続制御プログラムを記録したコンピュータ読取可能な記録媒体であって、

前記接続制御プログラムは、

前記通信制御サーバに、当該通信端末への接続が許可された通信端末の登録要求をする許可通信端末登録要求ステップと、

- 5 前記通信端末のネットワーク上におけるアドレスを特定するための宛先情報を要求した通信端末が前記通信端末への接続が許可された通信端末である場合に限り、前記通信制御サーバから送信される、前記宛先情報を要求した通信端末を認証するための認証情報を受信する認証情報受信ステップと、

- 10 前記宛先情報を要求した通信端末から、接続受入要求と当該通信端末を識別するための識別情報を受信する識別情報受信ステップと、

前記認証情報と前記識別情報とが一致するか否かを判定する判定ステップと、

- 15 前記認証情報と前記識別情報とが一致する場合に限り、前記宛先情報を要求した通信端末からの接続受入要求に基づく接続を許可する接続制御ステップと

を含むことを特徴とするコンピュータ読取可能な記録媒体。

18. 通信制御サーバとネットワークで接続された通信端末に用いる接続制御方法であって、

- 20 前記通信制御サーバに、当該通信端末への接続が許可された通信端末の登録要求をする許可通信端末登録要求ステップと、

- 前記通信端末のネットワーク上におけるアドレスを特定するための宛先情報を要求した通信端末が前記通信端末への接続が許可された通信端末である場合に限り、前記通信制御サーバから送信される、前記宛先  
25 情報を要求した通信端末を認証するための認証情報を受信する認証情報受信ステップと、

前記宛先情報を要求した通信端末から、接続受入要求と当該通信端末を識別するための識別情報を受信する識別情報受信ステップと、

前記認証情報と前記識別情報とが一致するか否かを判定する判定ステ



ップと、

前記認証情報と前記識別情報とが一致する場合に限り、前記宛先情報を要求した通信端末からの接続受入要求に基づく接続を許可する接続制御ステップと

5      を含むことを特徴とする接続制御方法。

10

15

20

25

図1

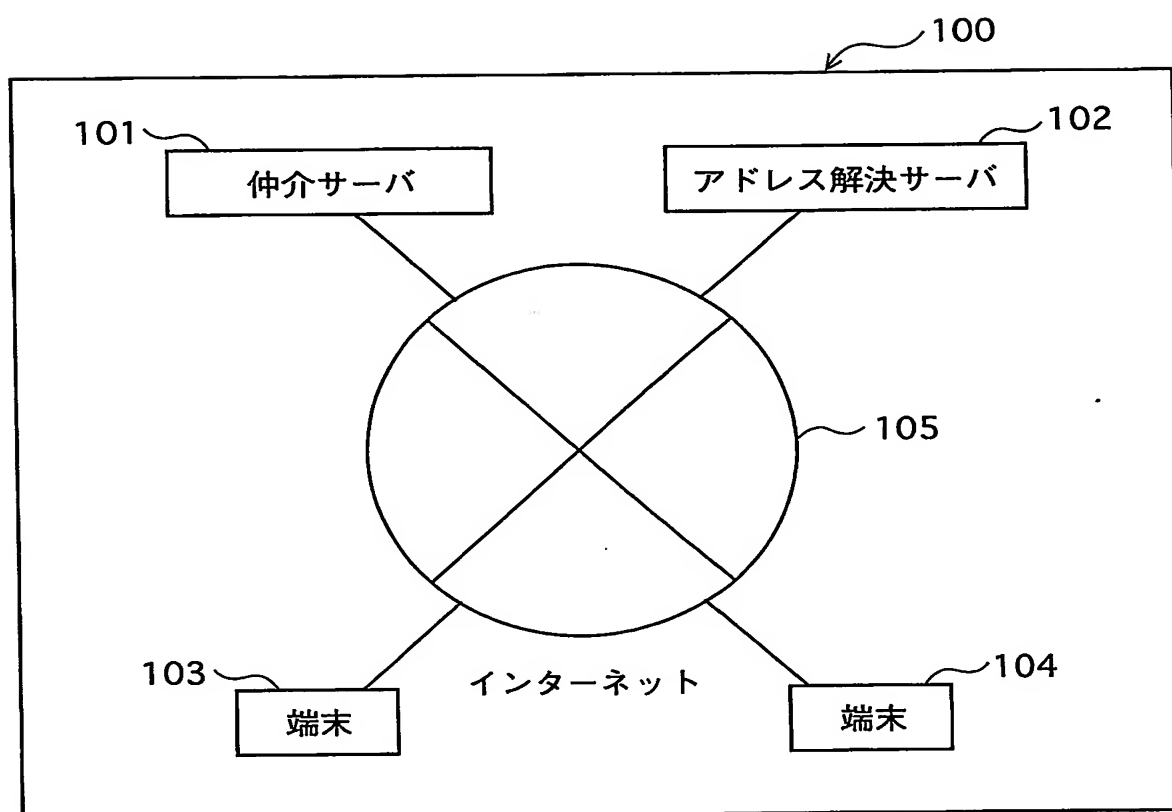


図2

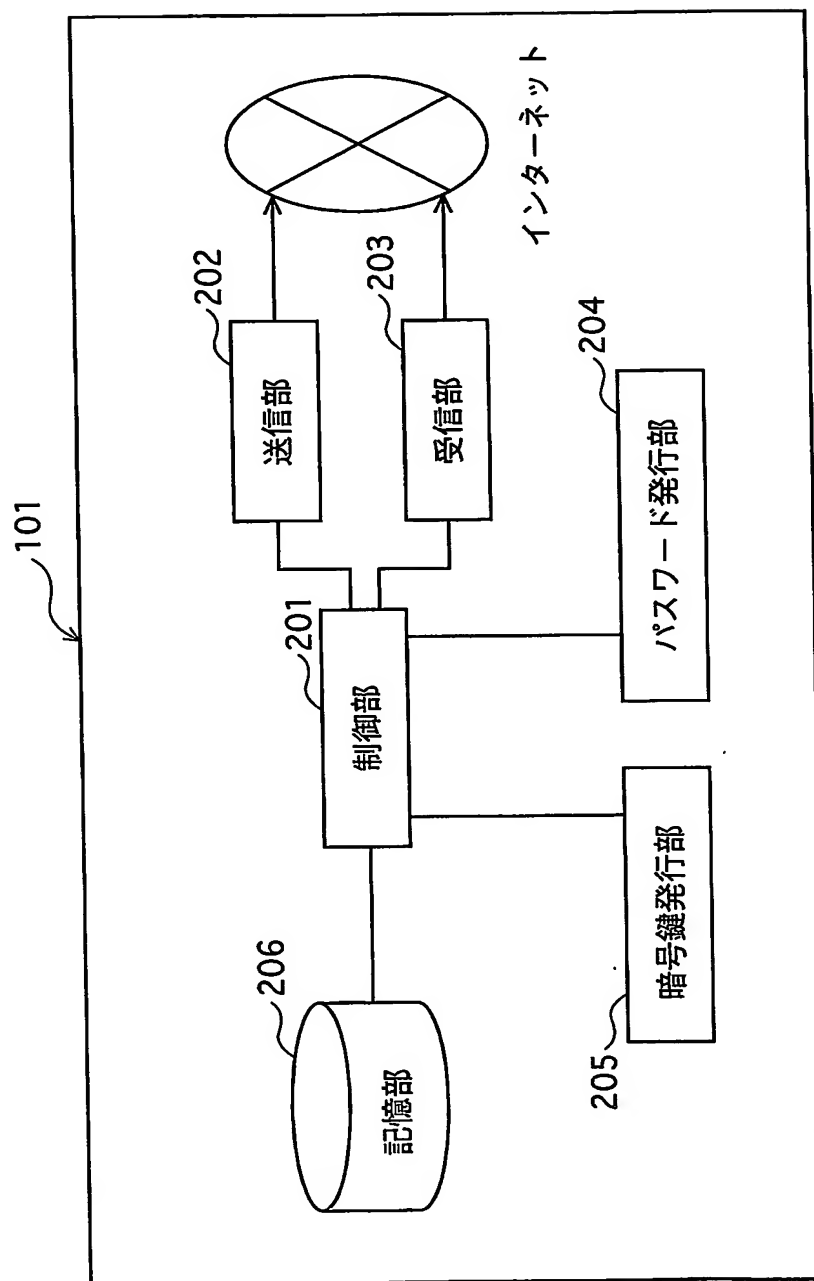


図3

(a)

REGISTER  
Identifier:la  
Accept:Create lb,lf

(b)

REGISTER  
Identifier:la  
Accept:Add lc,le

(c)

REGISTER  
Identifier:la  
Accept>Delete lf

(d)

REGISTER  
Identifier:la  
Accept:Add lc,le  
Delete lf

図4

端末の識別子	接続を受入れる端末の識別子
la	lb,lc,le
lb	la,lc,lf,lg

図5

(a)

QUERY  
Identifier:la  
Callee:lb

(b)

NOTIFY  
Request Accepted.

(c)

NOTIFY  
Permission Denied.

(d)

NOTIFY  
Callee Address:202.224.186.82  
Password:Password  
Encrypt Key:Key

(e)

NOTIFY  
Caller ID:la  
Password:Password  
Encrypt Key:Key

(f)

REQUEST  
Identifier:la  
Password:Password

(g)

NOTIFY  
Callee not Found.

(h)

NOTIFY  
Callee not Connected.

図6

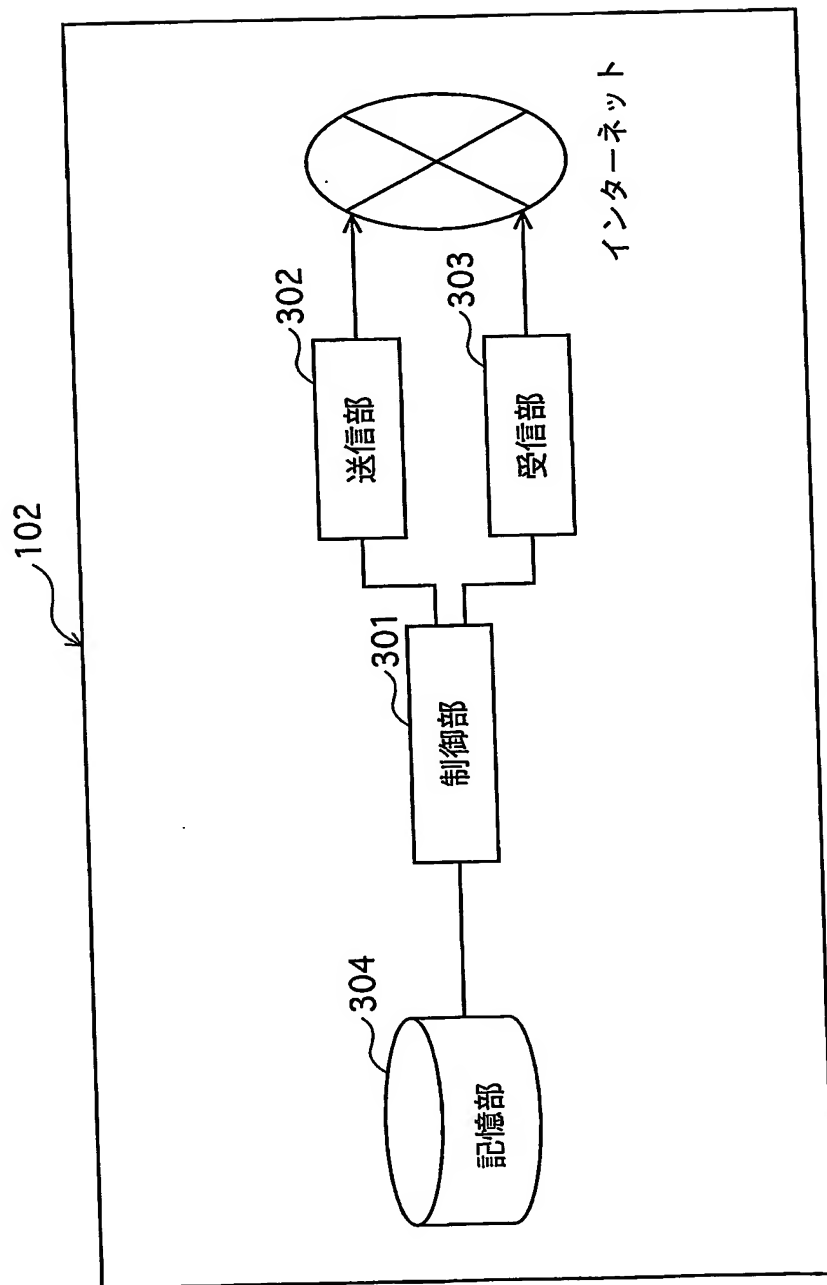


図7

端末の識別子	IPアドレス
la	202.224.186.81
lb	202.224.186.82



図8

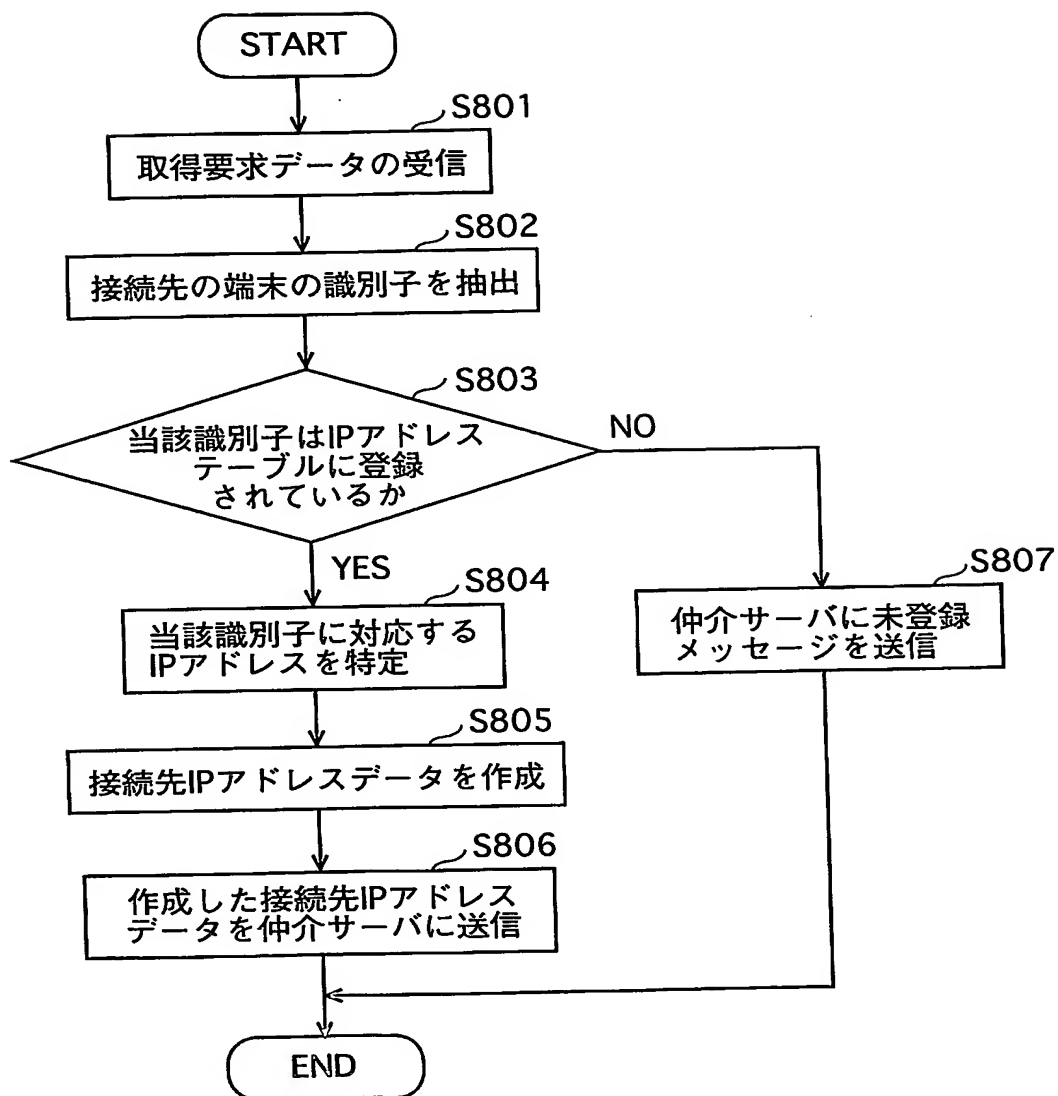


図9

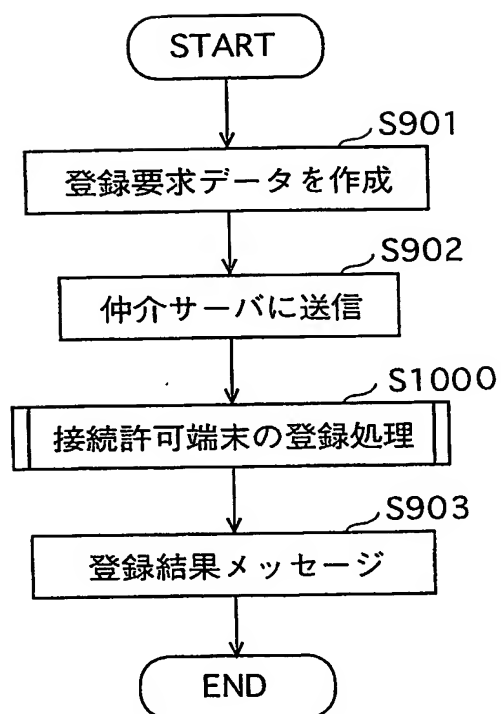


図10

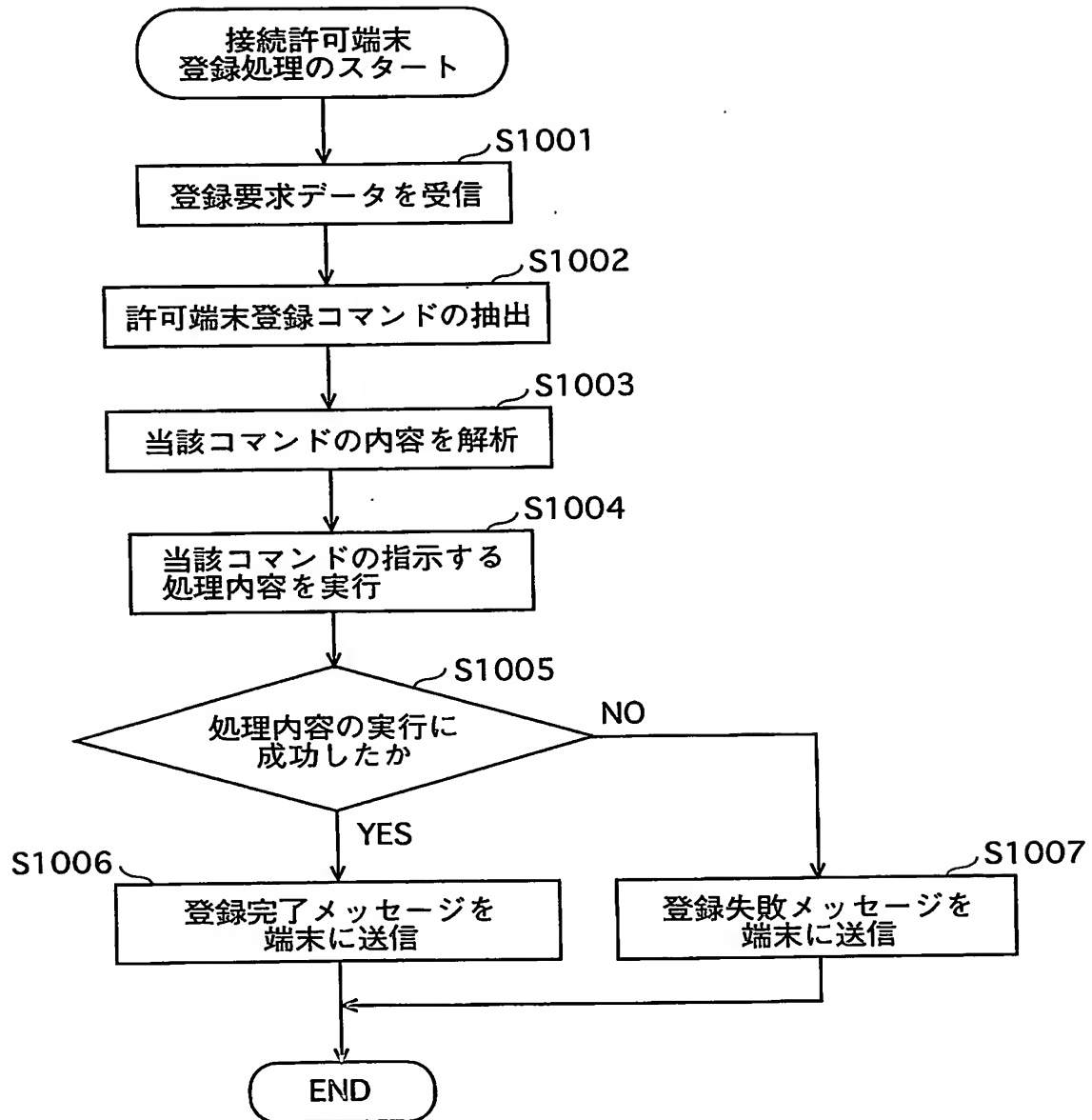


図11

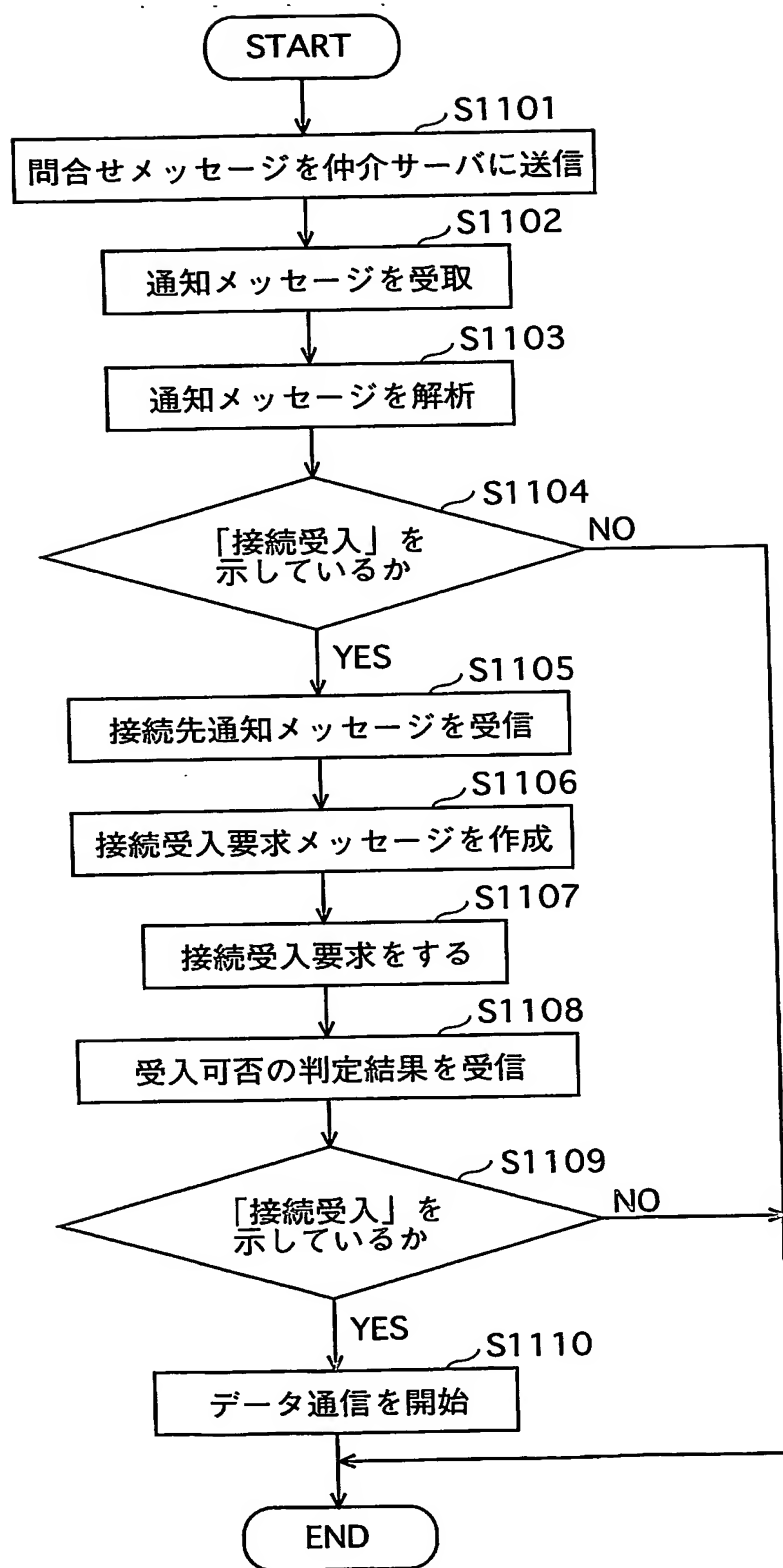


図12

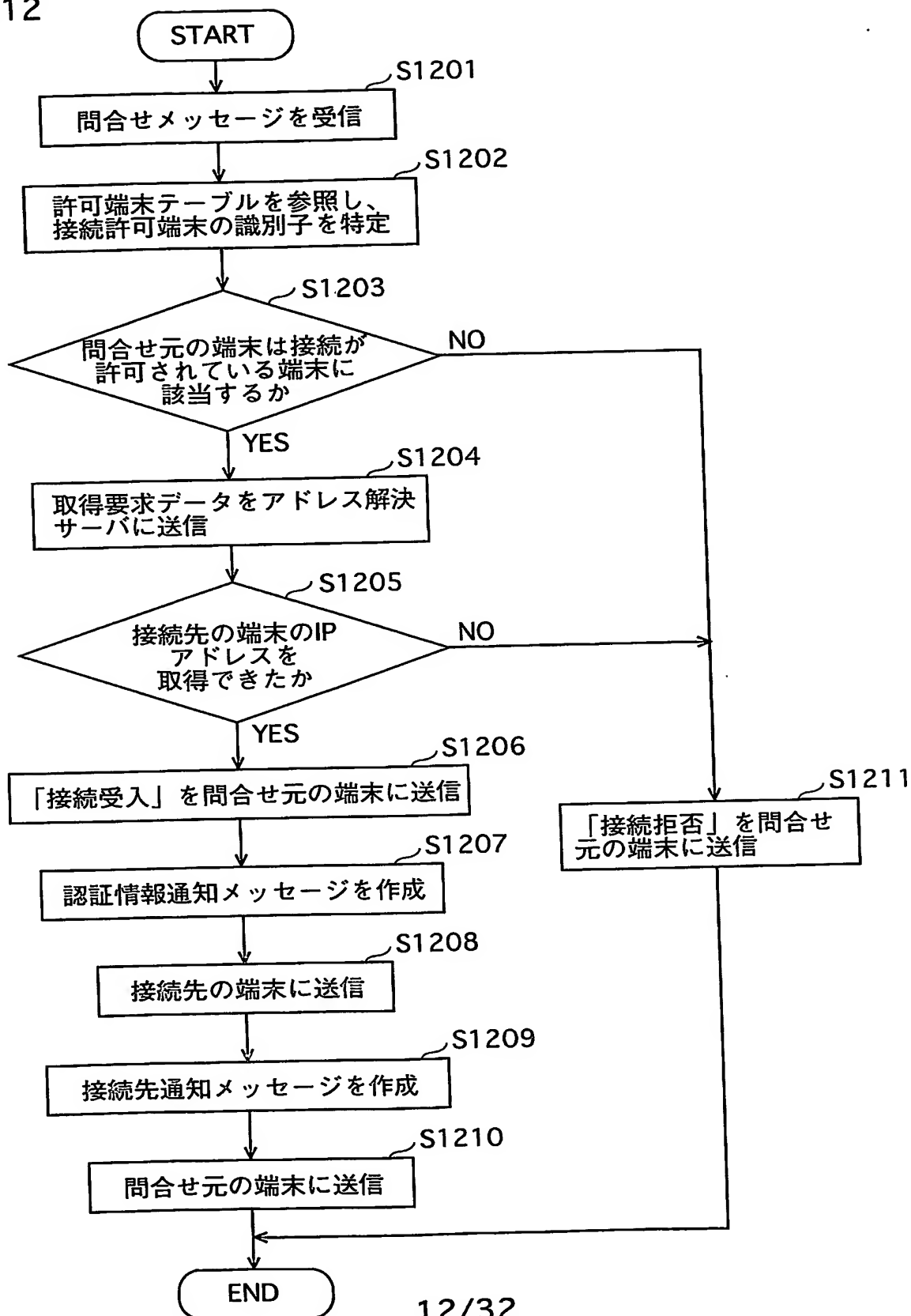


図13

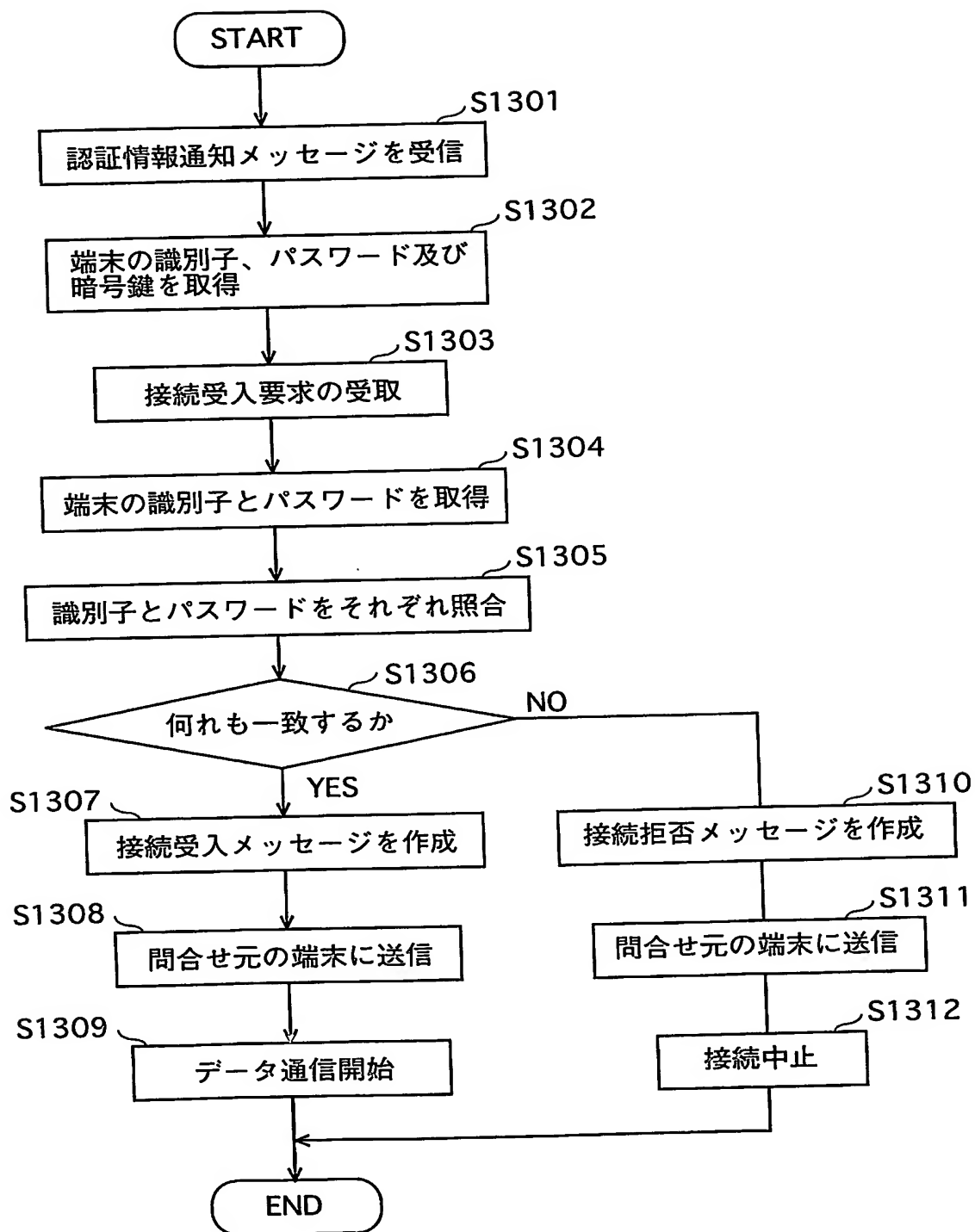


図14

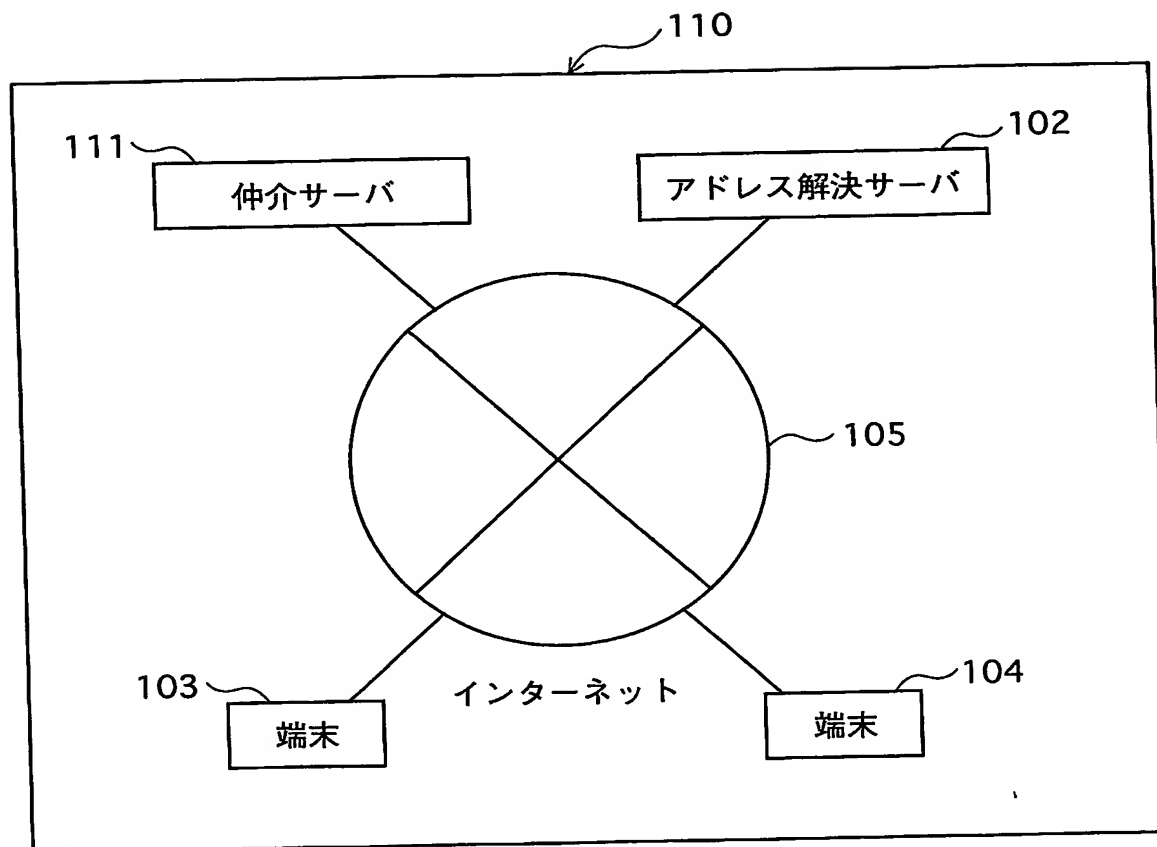


図15

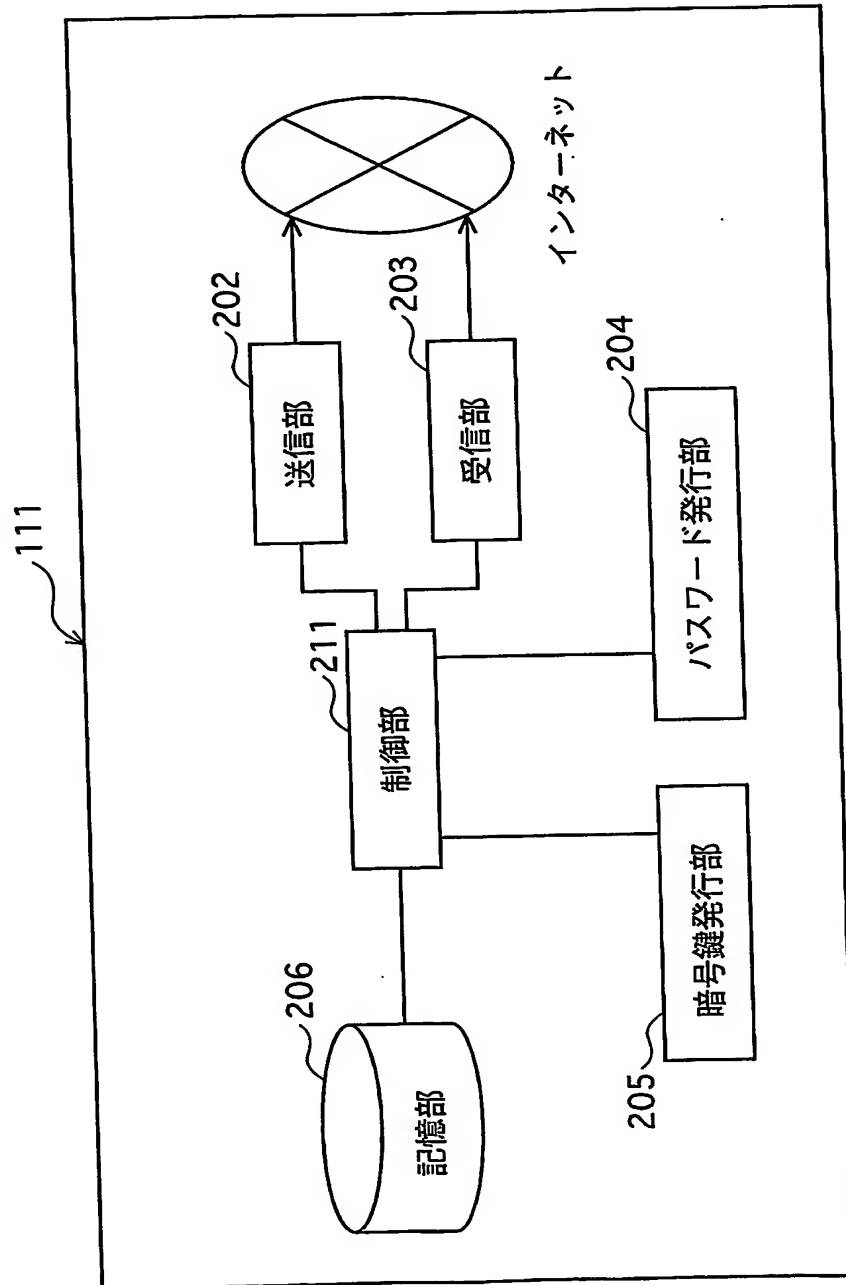
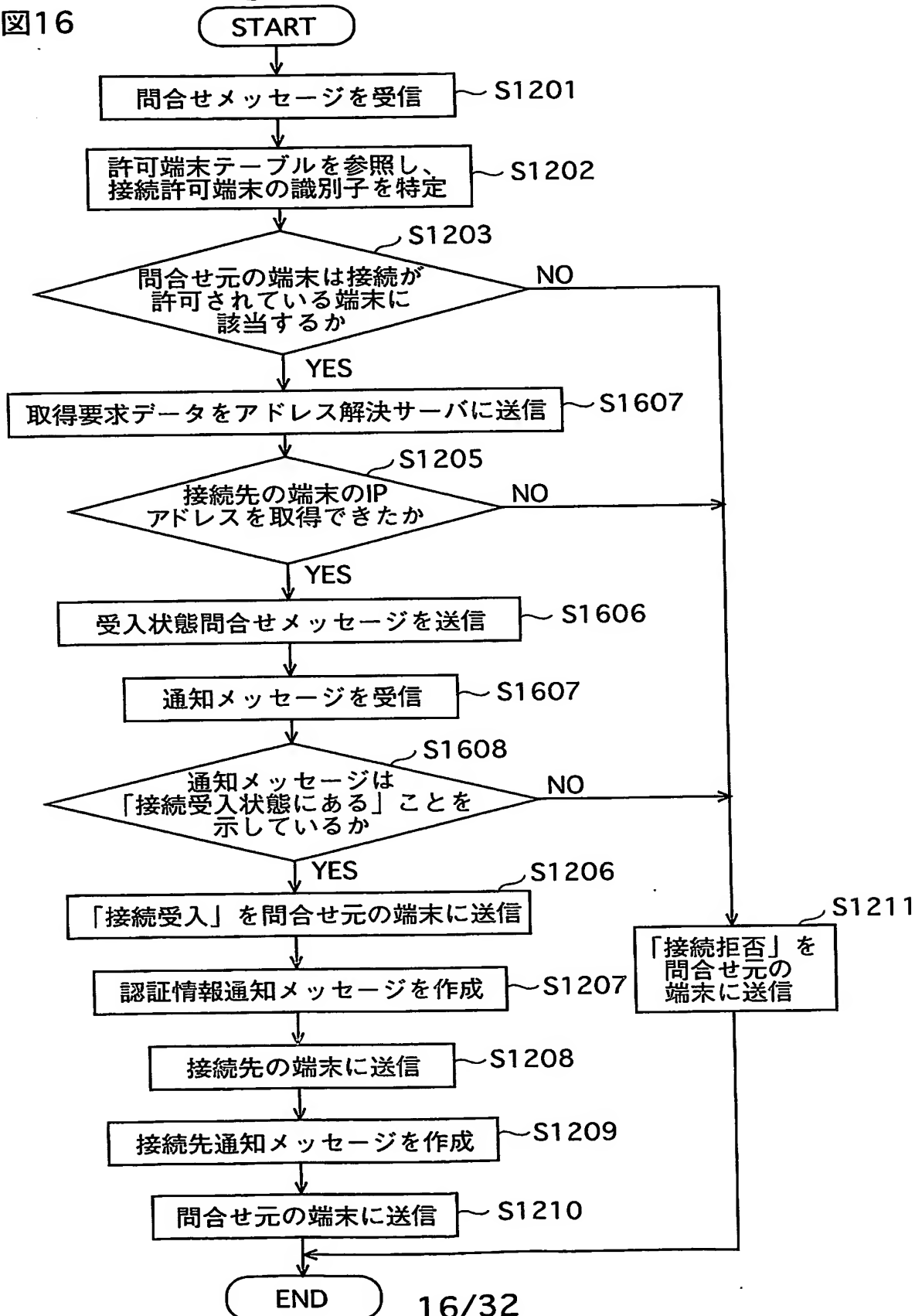




図16



☒17

(a)

QUERY  
STATUS

(b)

NOTIFY  
STATUS Acceptable.

(c)

NOTIFY  
STATUS Busy.

図18

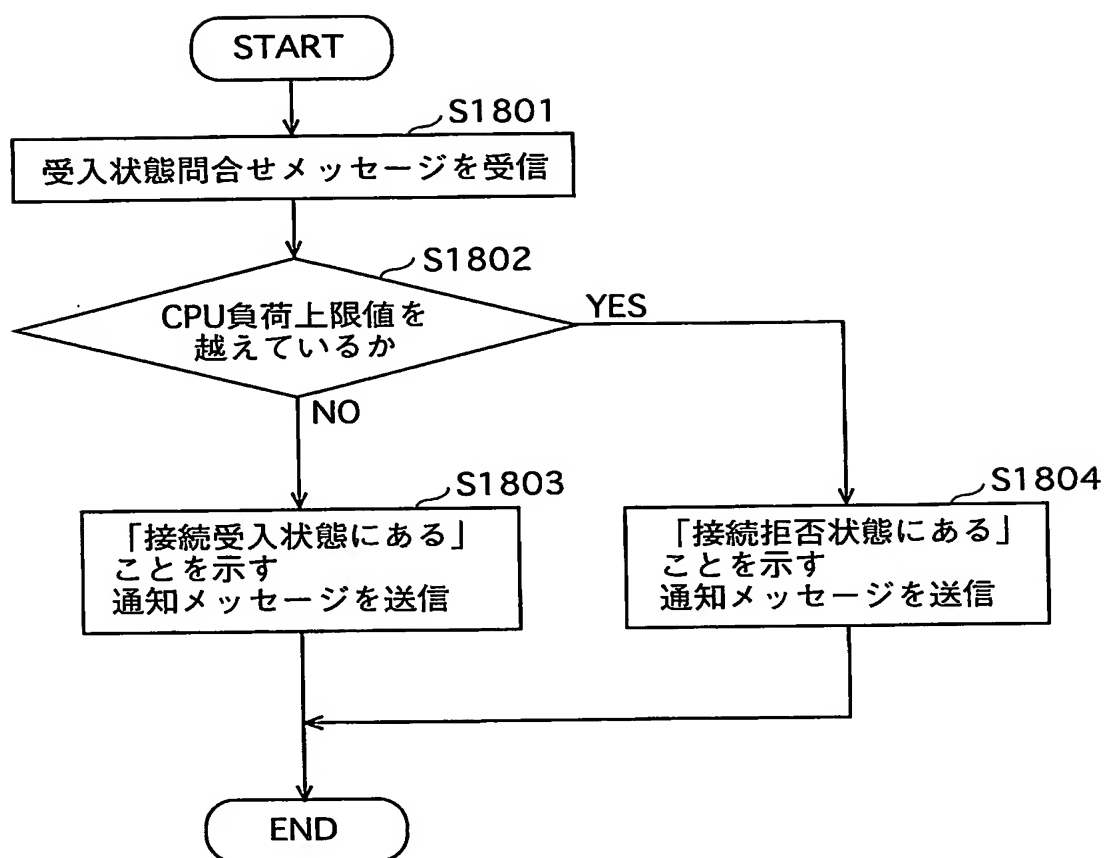


図19

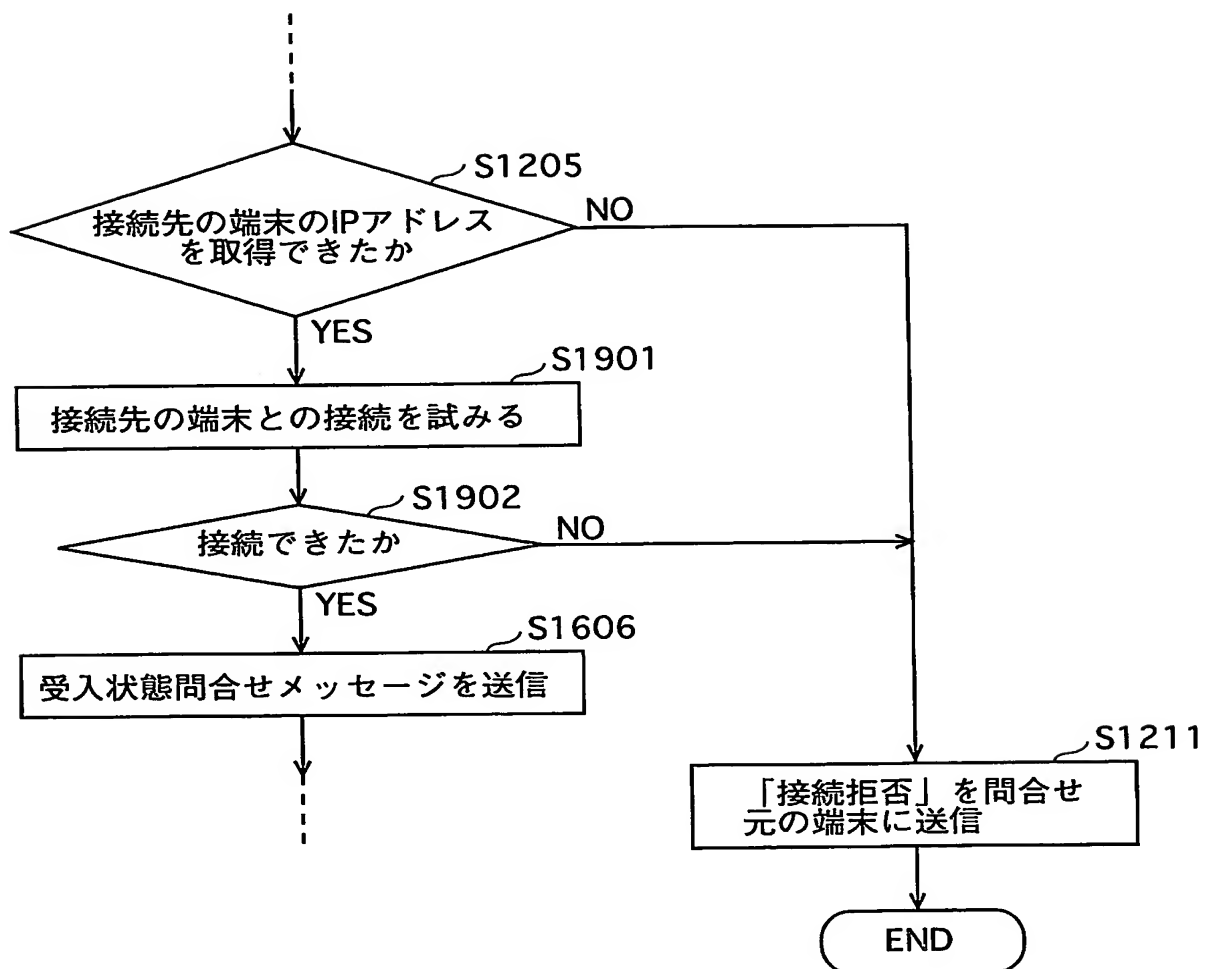


図20

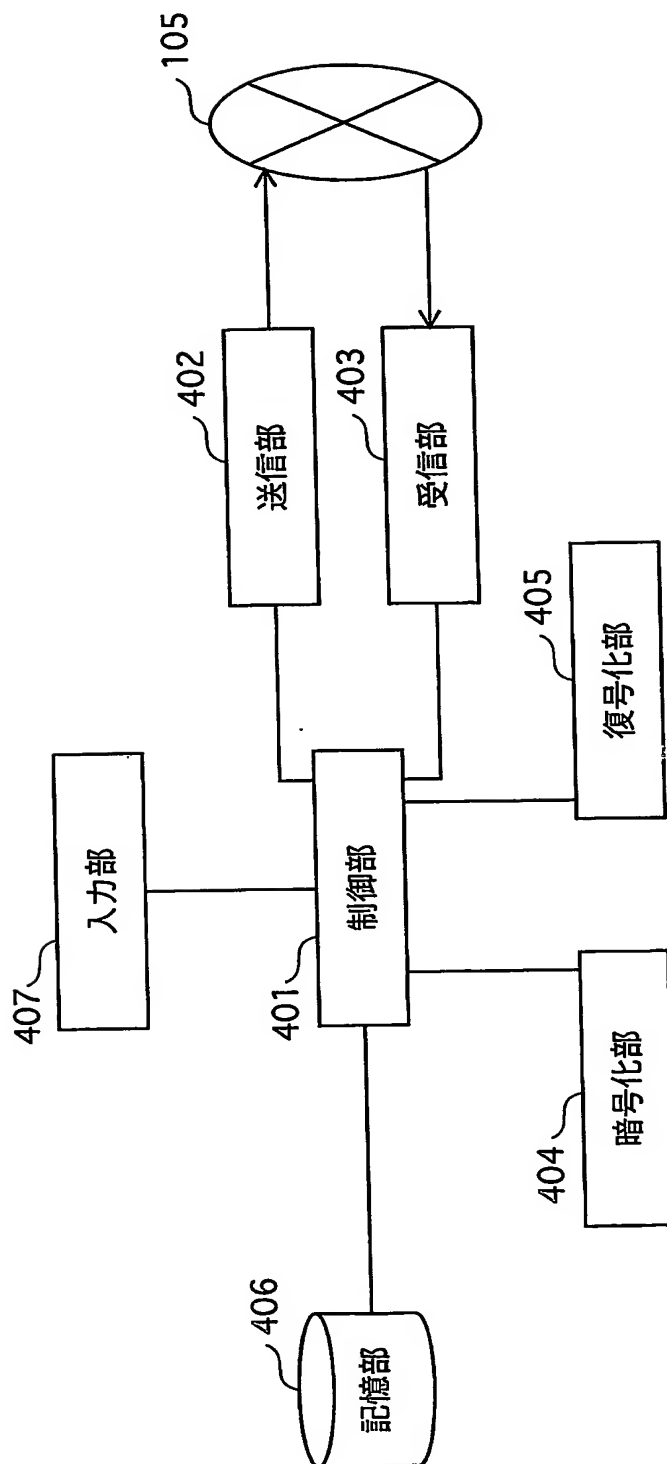


図21

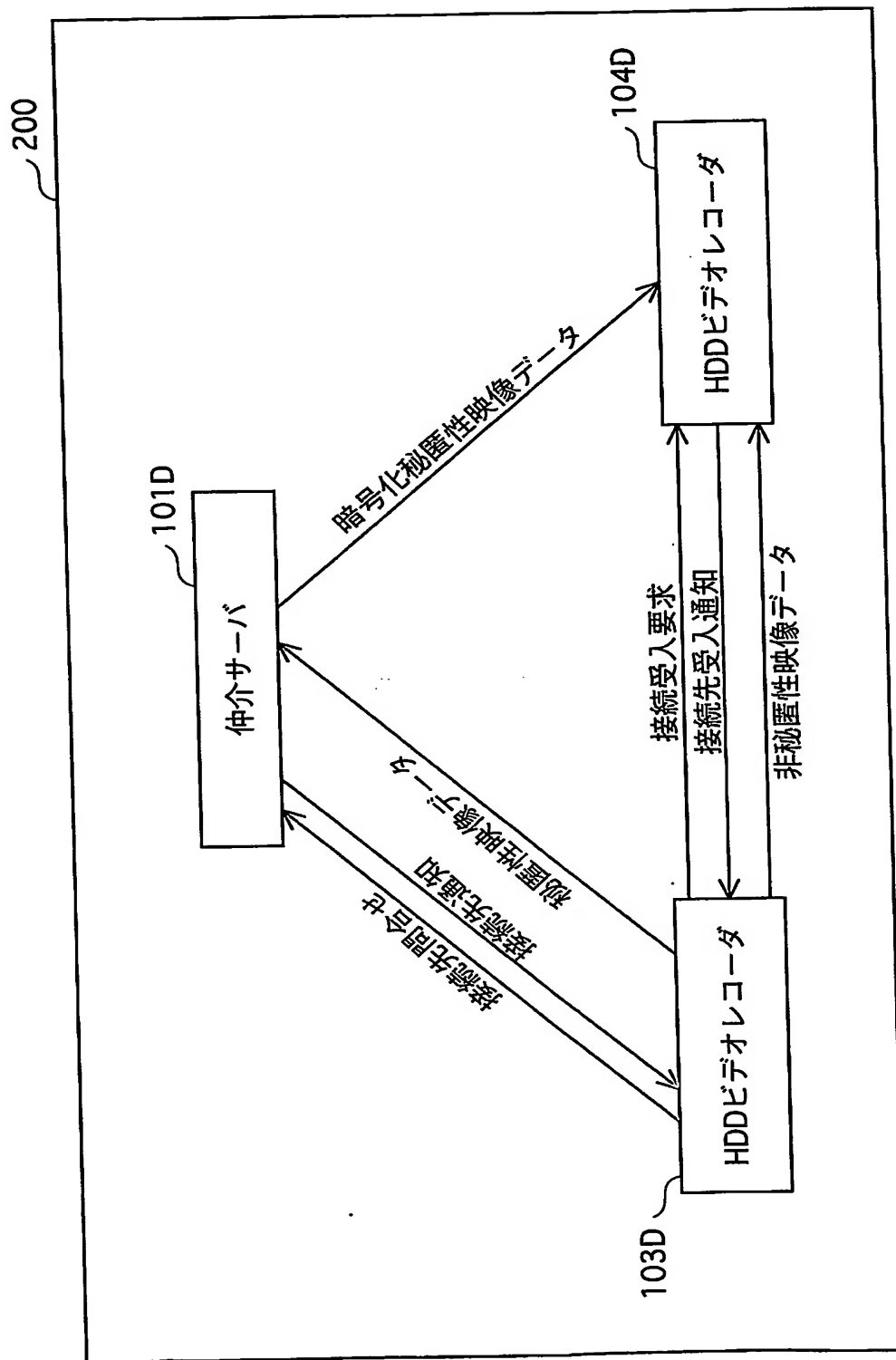


図22

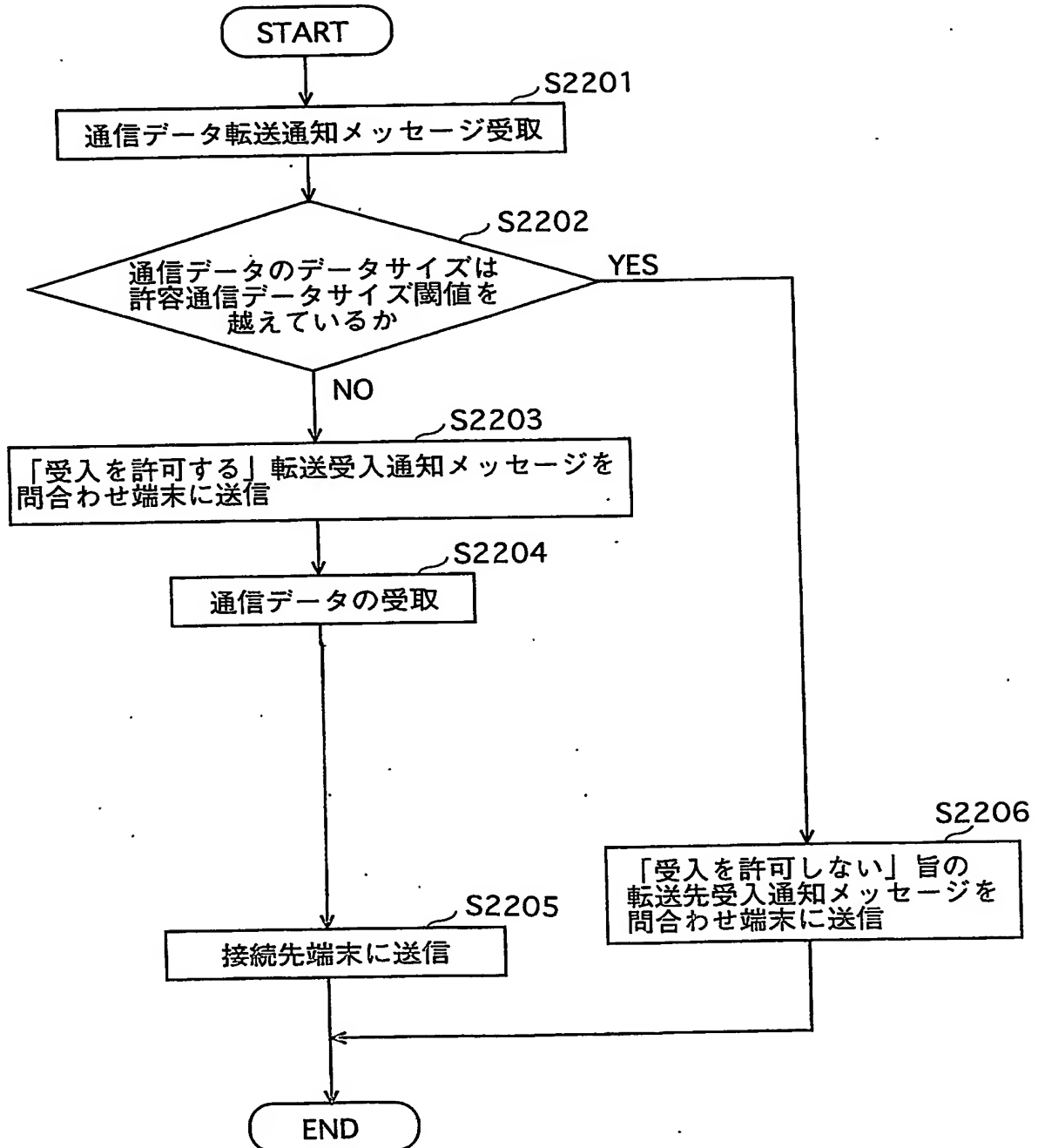


図23

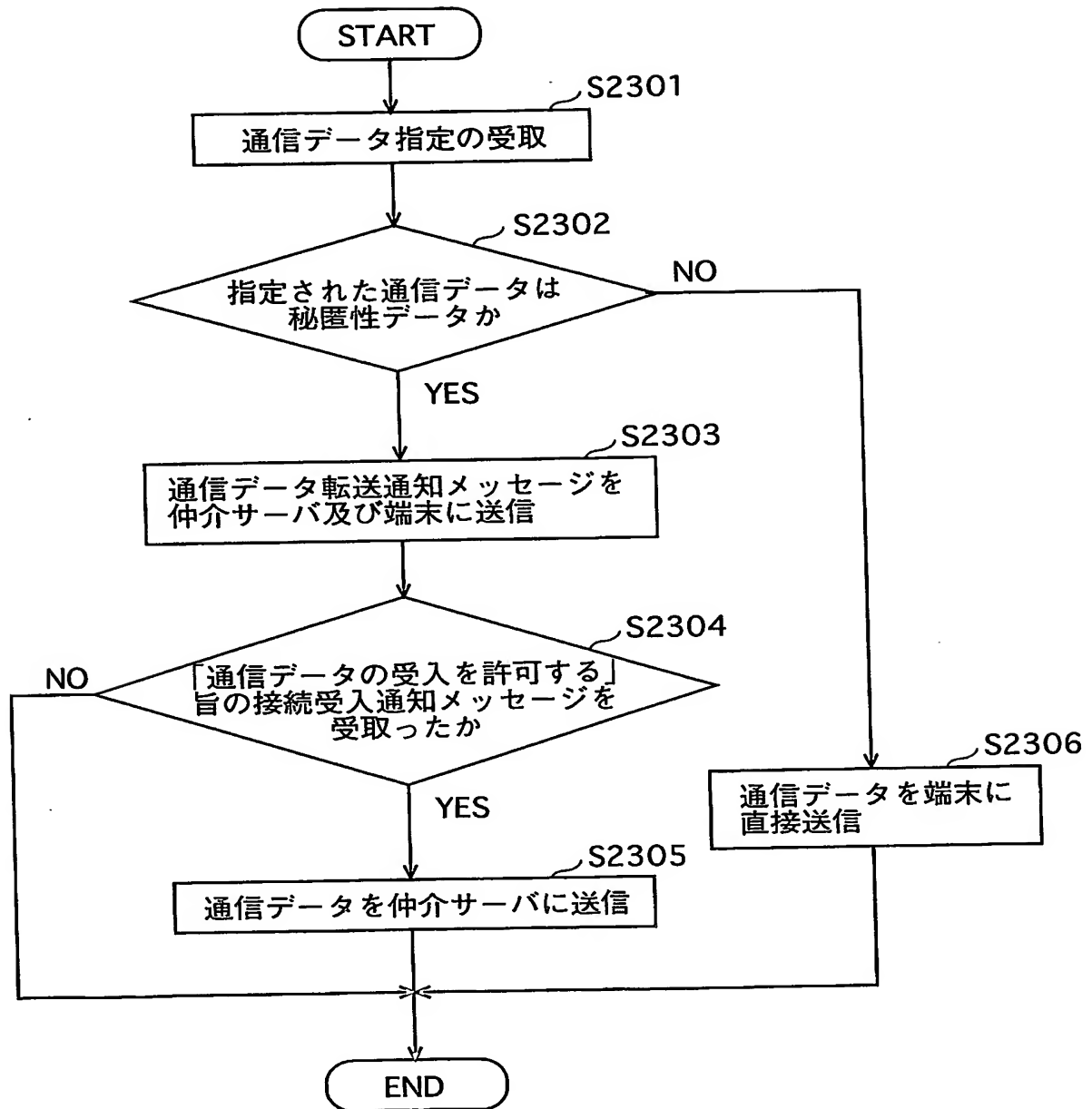




図24

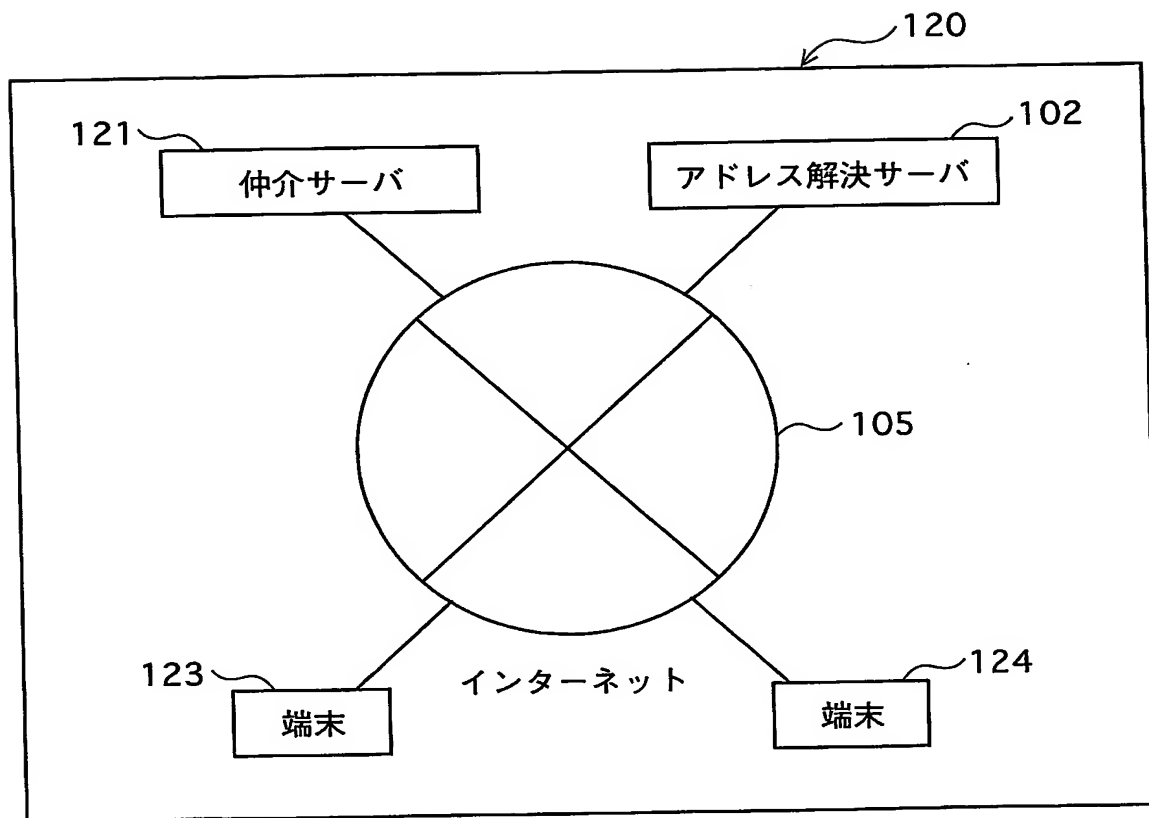


図25

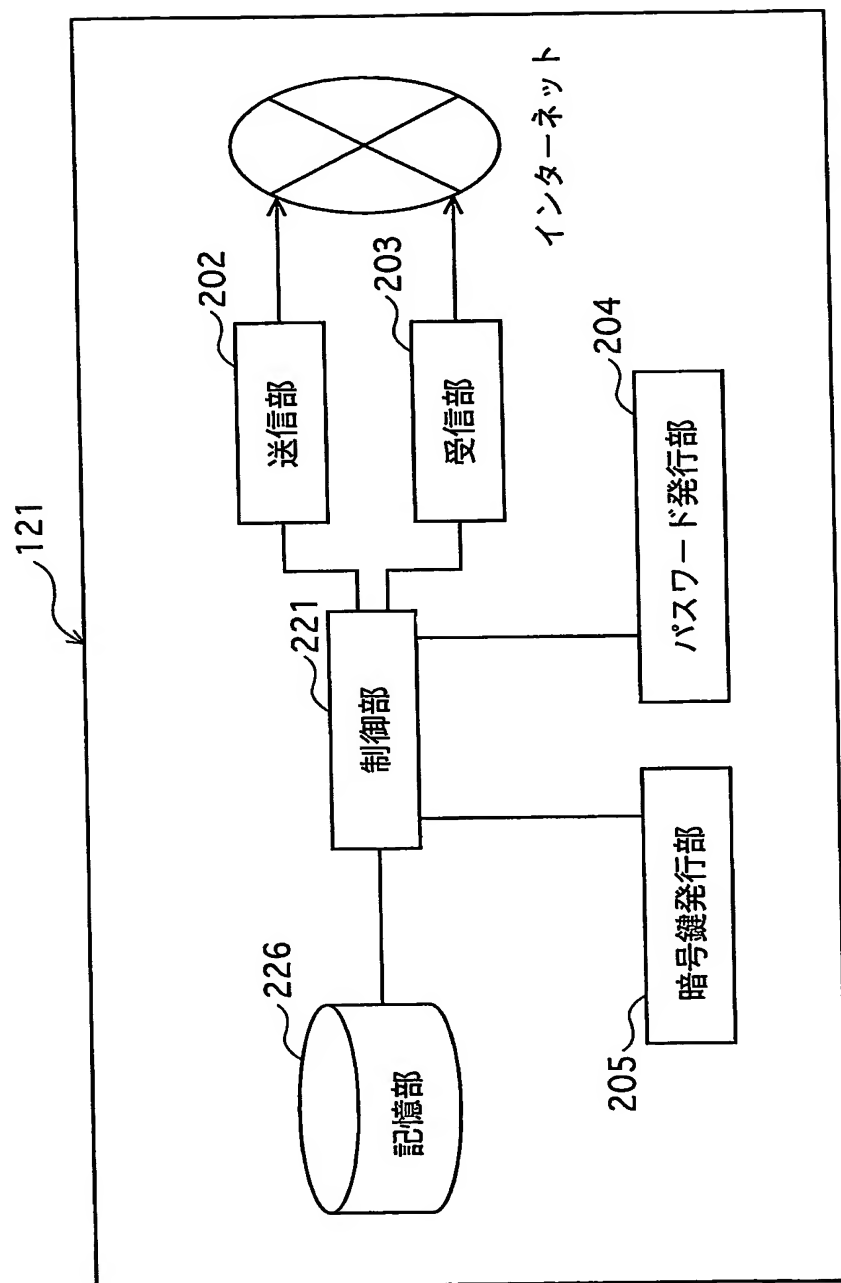


図26

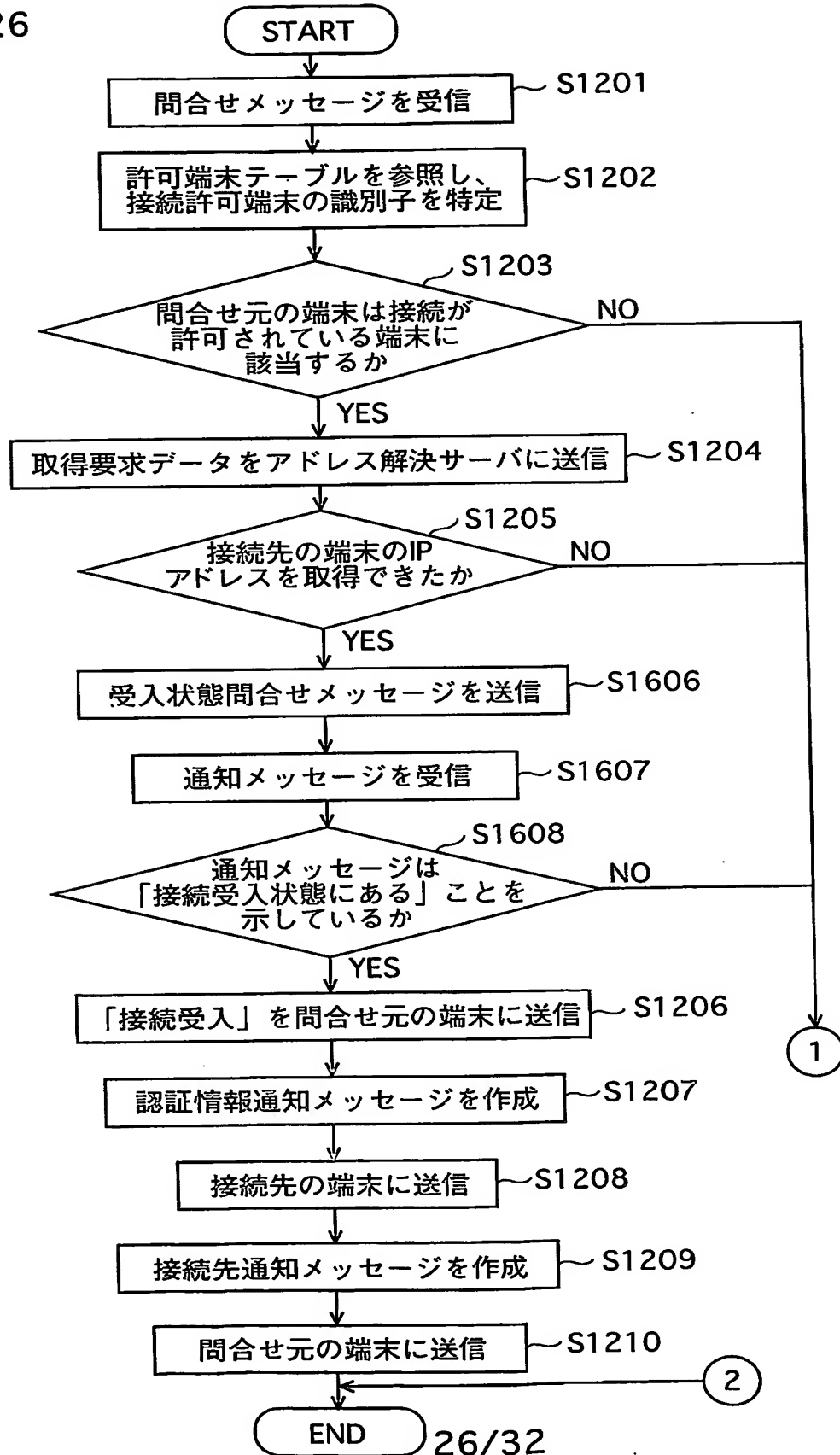


図27

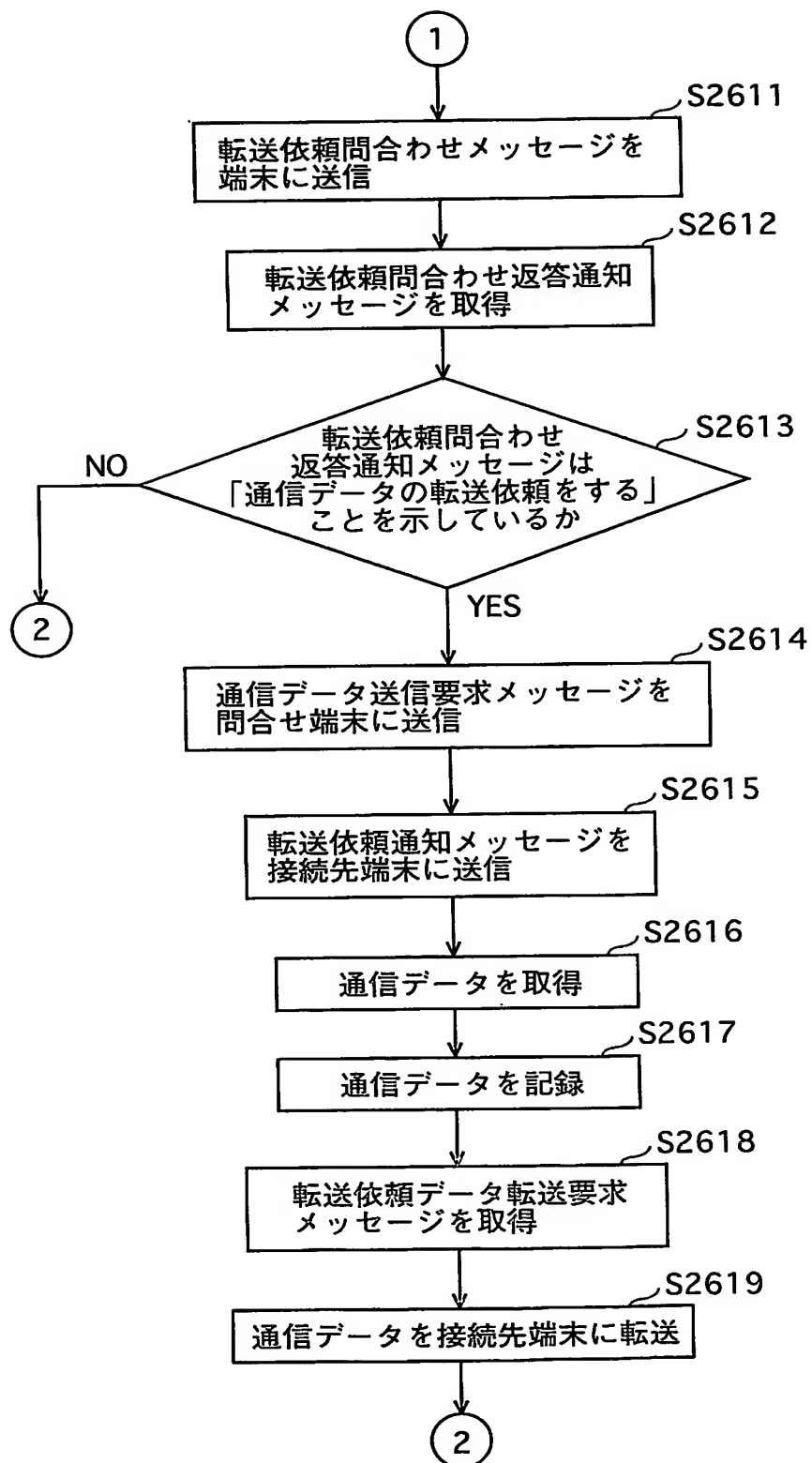


図28

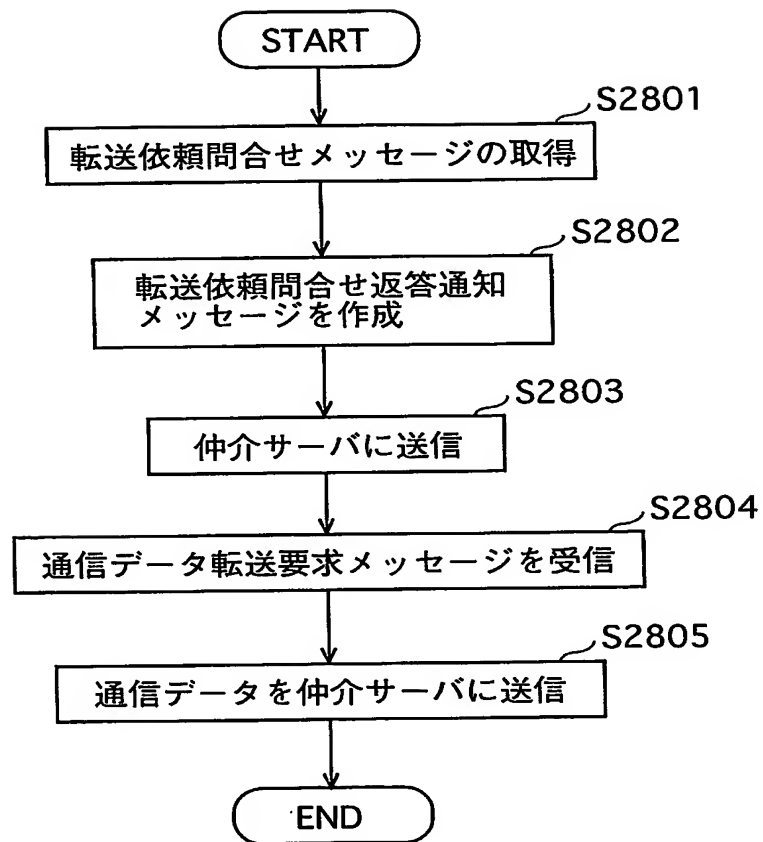


図29

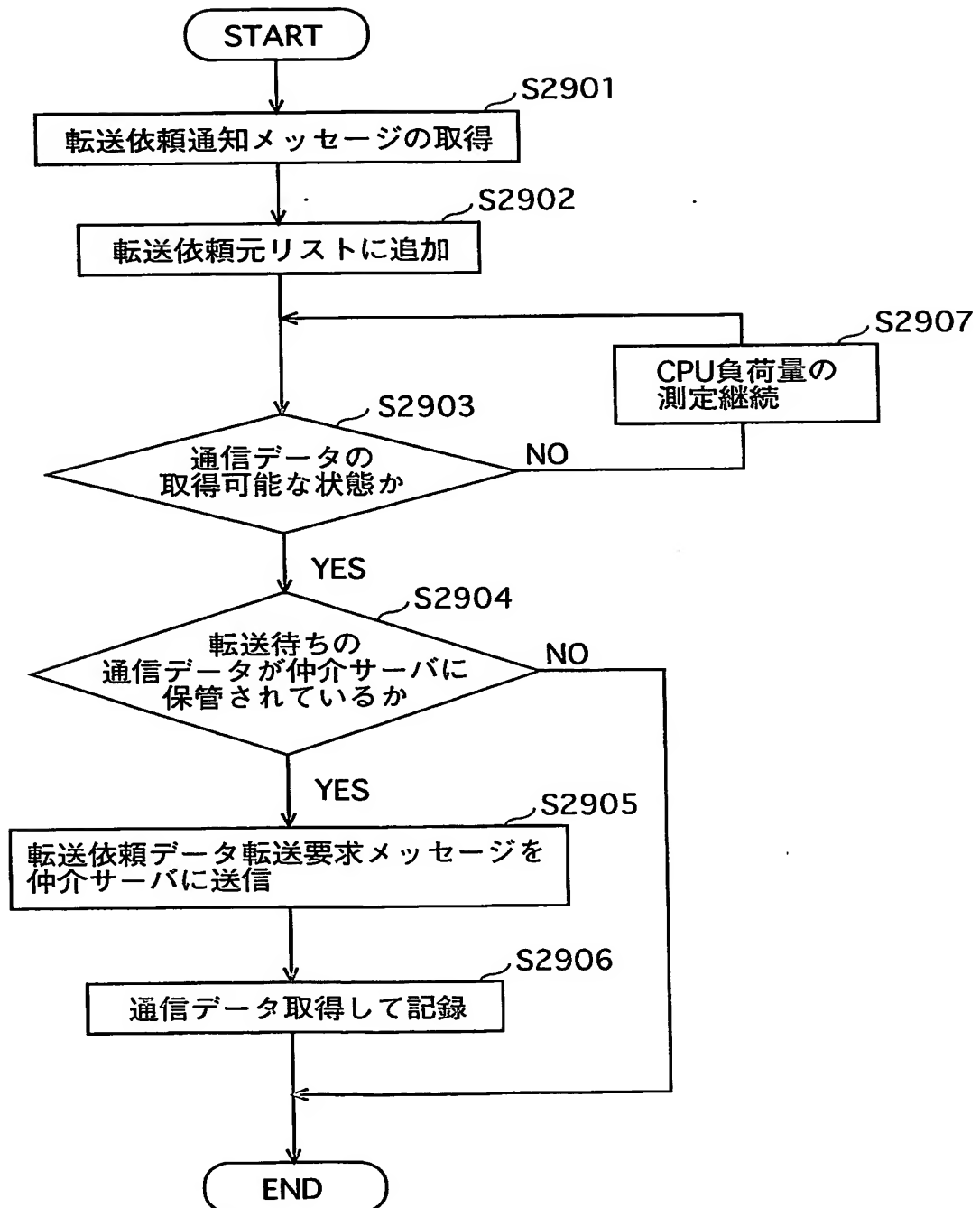


図30

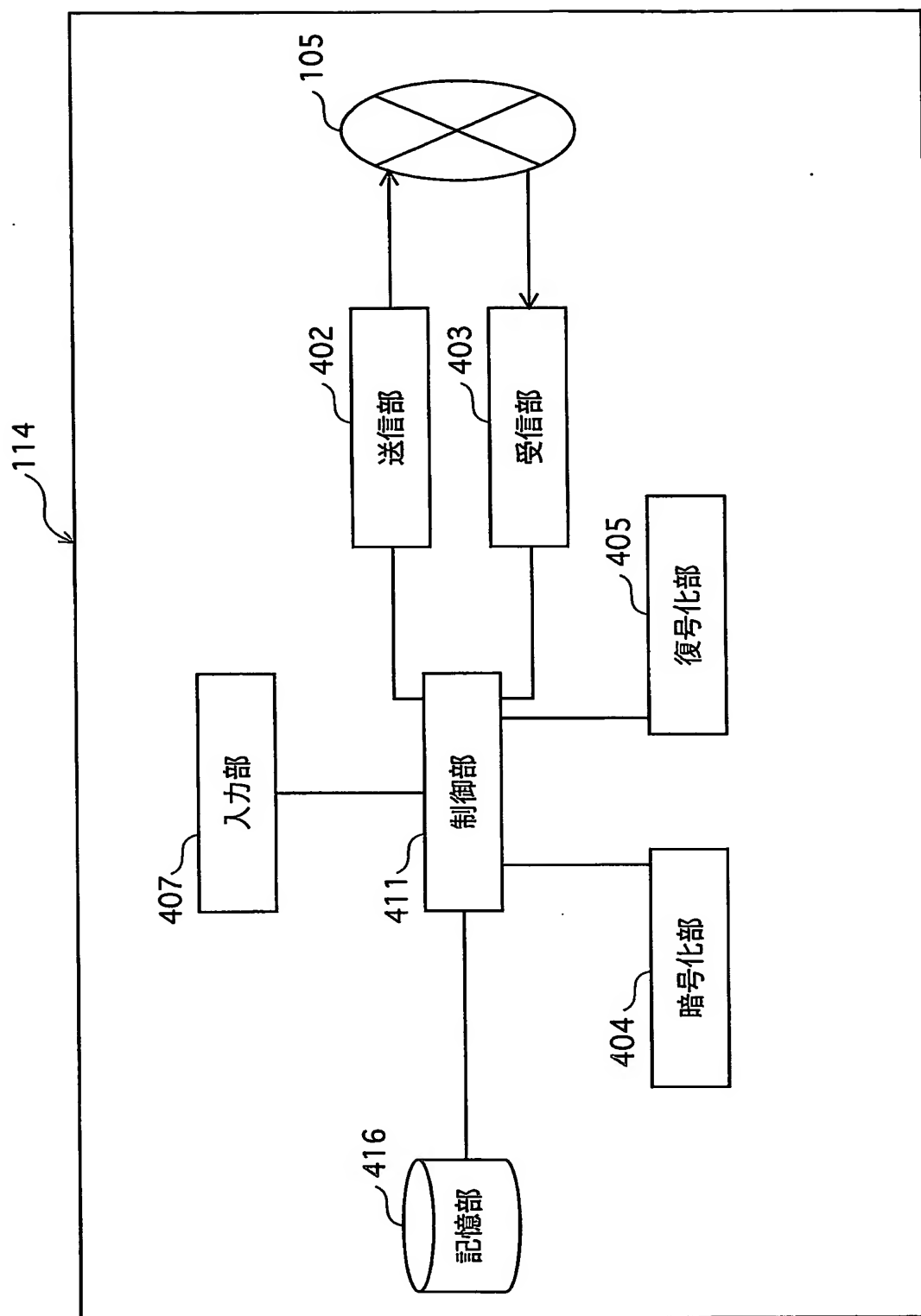


図31

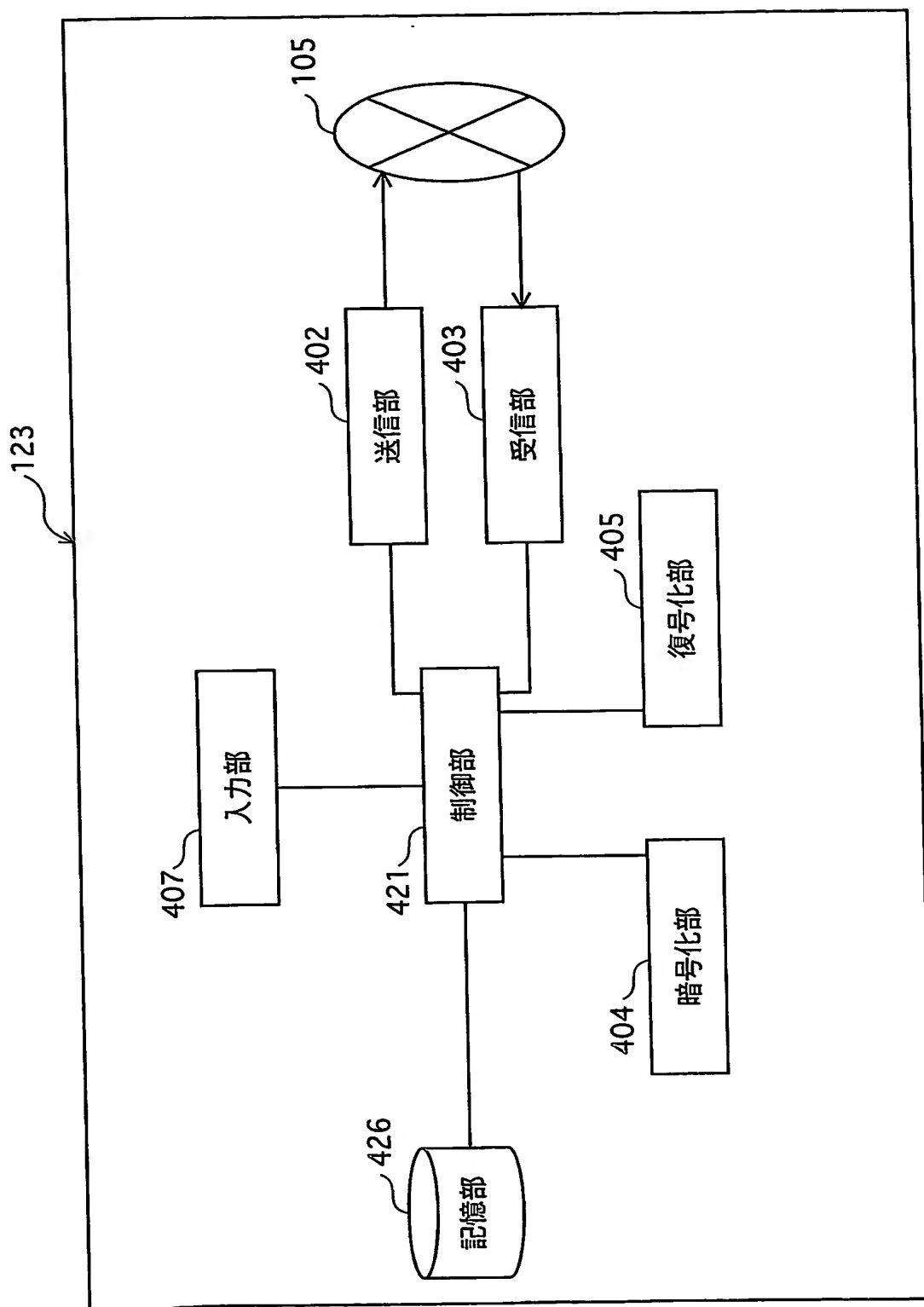
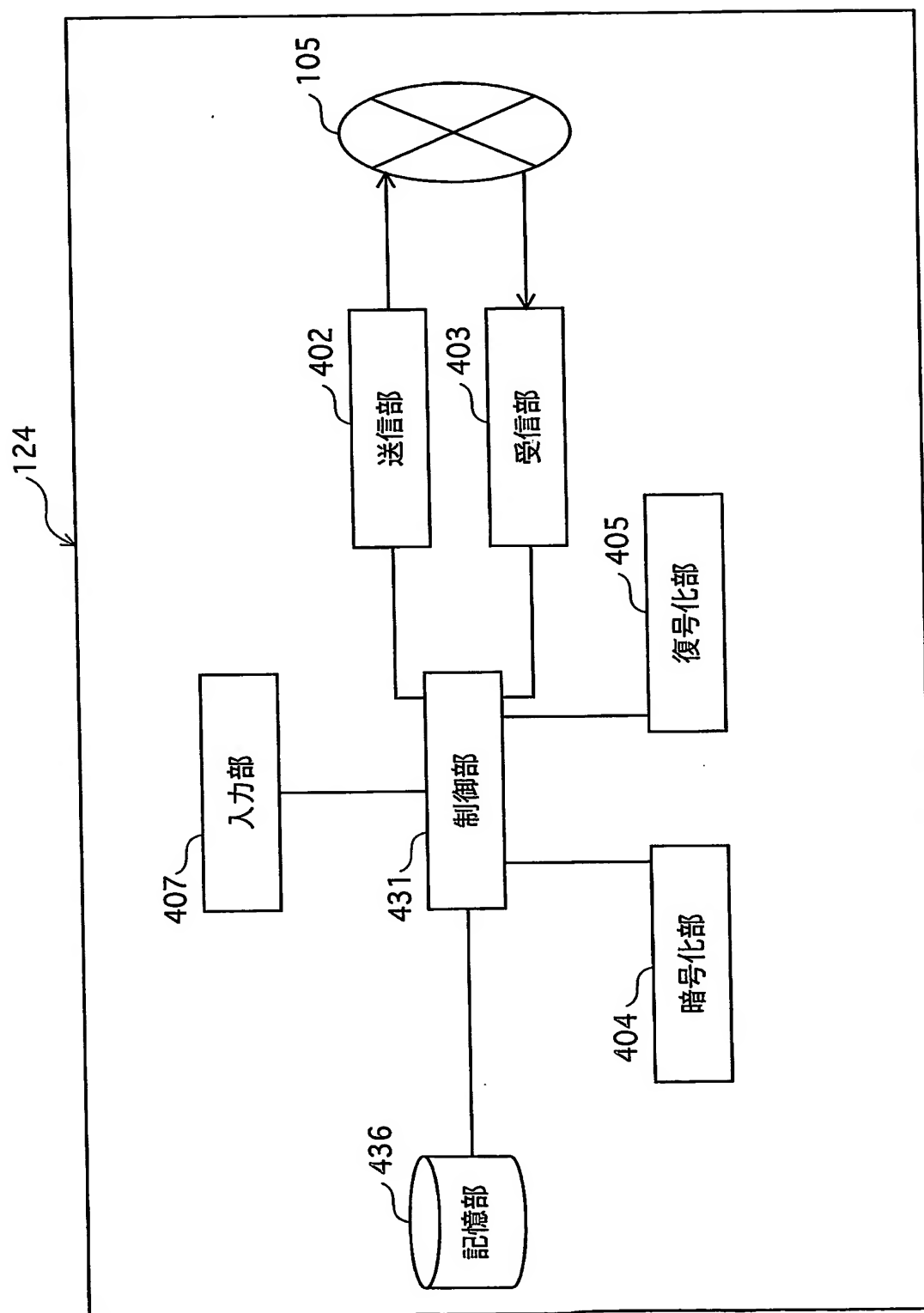




図32



## INTERNATIONAL SEARCH REPORT

Intern application No.

PCT/JP2004/001099

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> H041L2/66

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> H041L2/66, G09C1/00, H04L29/08, H04M11/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2002-199027 A (Kyocera Communication Systems Co., Ltd.), 12 July, 2002 (12.07.02), Par. Nos. [0001] to [0011], [0081] (Family: none)	1-9, 11-18 10
Y A	JP 2002-135457 A (Matsushita Electric Works, Ltd.), 10 May, 2002 (10.05.02), Par. Nos. [0009] to [0012]; Fig. 5 (Family: none)	1-9, 11-18 10

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search  
08 April, 2004 (08.04.04)Date of mailing of the international search report  
27 April, 2004 (27.04.04)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International Application No.

PCT/JP2004/001099

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 6-53956 A (NEC Home Electronics Ltd.), 25 February, 1994 (25.02.94), Par. No. [0007]; Fig. 1 (Family: none)	2, 4, 5, 7-9, 11
Y	JP 3-32269 A (NEC Corp.), 12 February, 1991 (12.02.91), Page 2, lower left column, line 15 to lower right column, line 3; Fig. 1 (Family: none).	4, 5, 7-9, 11
Y	JP 2002-368815 A (Matsushita Graphic Communication Systems, Inc.), 20 December, 2002 (20.12.02), Par. Nos. [0008] to [0013] & EP 1265429 A2 & US 2002/0194282 A1	8, 9, 11
A	JP 2002-208922 A (NTT Docomo Inc.), 26 July, 2002 (26.07.02), Par. No. [0056] & EP 1223706 A2 & US 2002/0118828 A1 & CN 1366395 A & KR 2002061115 A	10

A. 発明の属する分野の分類 (国際特許分類 (IPC))  
Int. Cl<sup>7</sup> H04L12/66

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L12/66 G09C 1/00  
H04L29/08  
H04M11/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
日本国公開実用新案公報 1971-2004年  
日本国登録実用新案公報 1994-2004年  
日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	JP 2002-199027 A (京セラコミュニケーションシステム株式会社) 2002. 07. 12 【0001】 - 【0011】; 【0081】 (ファミリーなし)	1-9, 11-18 10
Y A	JP 2002-135457 A (松下電工株式会社) 2002. 05. 10 【0009】 - 【0012】 , 図5 (ファミリーなし)	1-9, 11-18 10

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

\* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献  
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日  
08. 04. 2004

国際調査報告の発送日  
27. 4. 2004

国際調査機関の名称及びあて先  
日本国特許庁 (ISA/J P)  
郵便番号100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)  
玉木 宏治  
5X 3361  
電話番号 03-3581-1101 内線 3554

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P 6-53956 A (日本電気ホームエレクトロニクス株式会社) 1994. 02. 25 【0007】 , 図1 (ファミリーなし)	2, 4, 5, 7-9, 11
Y	J P 3-32269 A (日本電気株式会社) 1991. 02. 12 第2頁左下欄15行目~右下欄3行目, 図1 (ファミリーなし)	4, 5, 7-9, 11
Y	J P 2002-368815 A (松下電送システム株式会社) 2002. 12. 20 【0008】 - 【0013】 & EP 1265429 A2 & US. 2002/0194 282 A1	8, 9, 11
A	J P 2002-208922 A (株式会社エヌ・ティ・ティ・ドコモ) 2002. 07. 26 【0056】 & EP 1223706 A2 & US 2002/0118 828 A1 & CN 1366395 A & KR 200 2061115 A	10